АВТОНОМИЯ ЛИЧНОСТИ

№ 2(16) 2018 ISSN 2413-6379

В номере:

☑ *Махов С. Ю. АНАЛИТИКА БЕЗОПАСНОСТИ (учебное пособие)*

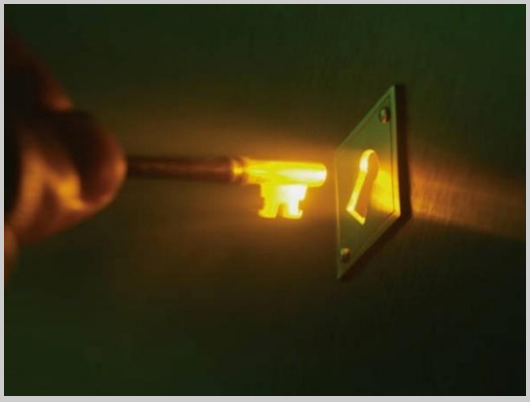
☑ *Кришталюк А. Н. ПРАВОВЫЕ АСПЕКТЫ СИСТЕМЫ БЕЗОПАСНОСТИ (курс лекций)*

☑ *Фирсова О. А. ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ (учебно-методическое пособие)*

АНАЛИТИКА БЕЗОПАСНОСТИ

СОДЕРЖАНИЕ

АНАЛИТИКА БЕЗОПАСНОСТИ

Махов С. Ю. 	АНАЛИТИКА БЕЗОПАСНОСТИ (учебное пособие)	3
Кришталюк А. Н. 	ПРАВОВЫЕ АСПЕКТЫ СИСТЕМЫ БЕЗОПАСНОСТИ (курс лекций)	118
Фирсова О. А. 	ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ (учебно-методическое пособие)	289

АНАЛИТИКА БЕЗОПАСНОСТИ

(учебное пособие)

В учебном пособии рассматривается широкий круг проблем по работе с разными по форме и содержанию источниками информации, обеспечению процесса подготовки и ведения аналитической работы.

Раскрываются принципы аналитической работы, структура и содержание этапов аналитической деятельности, последовательность поиска, анализа и методы изучения аналитической информации.

Предназначено, в первую очередь, тем, кто заинтересован в овладении теорией и практикой аналитической работы: преподавателям, аспирантам, руководителям и менеджерам организаций, сотрудникам правоохранительных органов и служб безопасности, сотрудникам аналитических служб и информационных отделов.

СОДЕРЖАНИЕ

Введение

ЧАСТЬ 1. АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БИЗНЕСА

Глава 1. Аспекты аналитического обеспечения безопасности

1.1. Требования к аналитику

1.2. Специфика теоретического познания и его формы

1.3. Аналитика – знание – информация

1.4. Процессы анализа и синтеза

1.5. Информационная аналитика

ЧАСТЬ 2. АНАЛИТИЧЕСКАЯ РАБОТА В СФЕРЕ БЕЗОПАСНОСТИ

Глава 2. Содержание аналитической работы

2.1. Анализ и основные понятия

2.2. Принципы аналитической работы

2.3. Применение логических законов в аналитической работе

2.4. Методы аналитической работы

Глава 3. Работа с источниками информации

3.1. Информация – основа успеха

3.2. Каналы информации

3.3. Обработка информации

3.4. Планирование работы

3.5. Поиск информации

3.6. Методы изучения документов

Глава 4. Оформление и использование аналитических результатов

Глава 5. Психологическая безопасность аналитической работы

Заключение

Литература

Введение

Современные методы управления предпринимательской деятельностью (менеджмент) ежедневно требуют новой информации о положении той или иной финансовой, деловой структуры на отечественном и международном рынке. Эти сведения (особенно, конфиденциальные) становятся товаром, который производится, помогая предпринимателю защитить свой бизнес от конкурентов, принять верное решение и выжить (до следующей схватки) в условиях жесткой конкуренции. Они же продаются и покупаются, вымогаются и похищаются для того, чтобы «раздавить» конкурента. Работу по обеспечению защиты и добыче информации в конкретных условиях рынка ведут различные как государственные, так и частные структуры: службы безопасности, детективные агентства, аналитические центры и т.д.

Аналитика в деле обеспечения безопасности предпринимательской деятельности все эффективнее внедряется в новое российское бытие. Аналитическая деятельность, когда-то бывшая уделом спецслужб, придворных политических обозревателей, ученых и т.д., активно встает на службу бизнесу, становится материальной движущей силой и защитой рыночной экономики. Элитарная сфера приложения человеческого интеллекта все больше привлекает к себе представителей бизнеса, различных структур безопасности.

Учитывая, что аналитическая деятельность по своей внутренней природе специфична, трудно говорить о практике её преподавания в обычном смысле слова. Многие специалисты сравнивают работу аналитика с творчеством ученого, исследователя, писателя, журналиста. Можно добавить, в ряде случаев – вместе взятых. Практика аналитической работы в безопасности бизнеса показывает, что аналитик должен: иметь развитый интеллект; обладать способностью к самосовершенствованию; знать специфику деятельности предприятия, учреждения, фирмы, банка; быть психологом; владеть писательским мастерством; работать (писать) в форс-мажорных обстоятельствах; и еще многое другое... Естественно, все эти обстоятельства нужно учитывать при разработке учебной программы, наборе слушателей и студентов, желающих посвятить себя профессии аналитика. Одновременно следует заранее предполагать, что конечный продукт учебного процесса не всегда окажется будущим аналитиком.

В данной работе нет попыток, охватить все стороны практической аналитики, поскольку аналитика как предмет еще требует своего всестороннего осмысления. Мы только попытаемся приоткрыть дверь в этот заманчивый мир творческого анализа для начинающих аналитиков. Для людей, которые хотят постичь азы науки мышления, устно и письменно правильно и четко излагать свои мысли. Уметь искать и находить нужную информацию, а поэтому познать нормы и правила человеческого общения. Испытать радость или горечь (последнее чувство обычное для начинающих аналитиков и в этом нет ничего зазорного) от процесса подготовки и выпуска в свет первого самостоятельного аналитического документа. Думаем, она вызовет интерес у руководителей предприятий, начальников и кадровиков служб безопасности и организаций, которые постоянно испытывают трудности с приемом на работу квалифицированных аналитиков. Да многие кадровики и не представляют себе, какие же кадры нужны для аналитики, какие требования предъявлять к кандидатам на данную профессию. А время учить и учиться аналитике уже наступило.

ЧАСТЬ 1
АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ БИЗНЕСА

Глава 1. Аспекты аналитического обеспечения безопасности

1.1. Введение в аналитику

Сложность современной аналитической деятельности заключается в том, что система обеспечения безопасности нынешнего бизнес-процесса требует для своего анализа профильных специалистов-аналитиков: математиков, статистиков, социологов, психологов. Но только аналитики с широким экономическим, политическим, социальным, оперативным кругозором на основе информации, полученной от данных сотрудников, могут предоставить потребителю понятный ему окончательный аналитический документ, сделать выводы из аналитического материала, дать перспективное видение проблемы, спрогнозировать дальнейшее развитие событий и иметь варианты выхода из виртуального кризиса.

Учитывая, что аналитическая деятельность по своей внутренней природе специфична, трудно говорить о практике её преподавания в обычном смысле слова. Многие специалисты сравнивают работу аналитика с творчеством ученого, исследователя, писателя, журналиста. Можно добавить: в ряде случаев – вместе взятых.

Практика аналитической работы в СБ показывает, что аналитик должен:

- иметь развитый интеллект (от природы),

- обладать способностью к самосовершенствованию (характер, практика),

- знать специфику деятельности предприятия, учреждения, фирмы, банка (учеба, практика),

- иметь представление об оперативной работе (учеба, практика),

- быть психологом (учеба, практика),

- владеть писательским мастерством (талант, учеба, практика),

- работать (писать) в форс-мажорных обстоятельствах (характер, практика),

- и еще многое другое...

Интеллектуальные способности аналитика – это его «визитная карточка». Оригинальность и логика мышления, энциклопедические знания всегда были в цене. Интеллект (ум, рассудок, познание, разумение) – способность мышления,

рационального познания, система умственных операций, индивидуальный стиль и стратегия решения проблем, врожденная и приобретенная на практике адаптация к разным жизненным ситуациям. Интеллектом наделен каждый человек. Не каждый стремится развить его. Развитие интеллекта – это тренировка внимания, памяти, мышления, психического состояния, воспитание трудолюбия, именно тех качеств, которые необходимы в повседневной работе сотрудников и аналитиков СБ. По мнению психологов, важнейшими признаками аналитического интеллекта являются:

- глубина – способность проникать в сущность событий и фактов, понимать их причины и закономерности, взаимосвязи и перспективы развития,

- критичность – объективная оценка фактов и явлений, стремление подвергать сомнению устоявшиеся взгляды, мнения, решения,

- гибкость – способность переключаться с одной идеи на другую, в том числе противоположную собственной,

- широта ума – способность видеть взаимосвязи явлений, объемное видение проблем,

- быстрота – скорость решения задач,

- оригинальность – способность находить неординарные решения, порождать новые идеи, отличные от общепринятых взглядов,

- пытливость – стремление доходить до самой глубинной сути событий,

- интуиция – способность предвидеть ход событий, после активного включения в работу всех признаков интеллекта.

Психологические качества аналитика СБ:

- уверенность в том, что выбор профессии правильный (чувство собственной удовлетворенности помогает карьере),

- умеренный профессиональный снобизм обязателен,

- усидчивость, педантичность (рутинная повседневная работа по ведению досье, пополнению банка данных, подшивок СМИ и т.д. часто надоедает, но является обязательным условием аналитического процесса),

- знание методов и способов концентрации мыслительного процесса в нужный момент (умение отключиться от всех проблем, сосредоточиться на внимательном изучении и анализе имеющейся информации, работа – прежде всего),

- умение отвлечься на время от исследуемой проблемы (важный момент, во время которого, отдохнувший мозг может «неожиданно» выдать интересные идеи),

- полет фантазии – (вопросы типа: «а что, если?» постоянно присутствуют в процессе написания аналитического документа, любые фантастические предположения обостряют чувство реальности),

- высокопарно – литературный дар, писательский талант (аналитик, обладающий писательским даром, ценится в СБ на вес золота),

- способность выработать свой стиль написания документа (приходит с годами, помогает руководителю СБ. учить молодежь на положительных примерах),

- умение менять стиль написания документа в зависимости от его содержания (политический портрет, экономический обзор, например, требуют разных стилей изложения),

- умение работать «в команде» (качество, необходимое при написании коллективных аналитических документов),

- способность профессионально отстаивать свою точку зрения (если руководство СБ сомневается в выводах, нужно уметь доказать правоту аналитических выводов и отстоять свою точку зрения на исследуемую проблему в определенных личными отношениями рамках, тогда уверенность, опыт и аналитические способности будут оценены по заслугам),

- объективная самокритика (но не самоунижение, понимание того факта, что ты – не есть истина в последней инстанции),

- здоровая (белая) профессиональная зависть (надежное качество, побуждающее к самосовершенствованию),

- стремление к постоянному самосовершенствованию (отход от узкой специализации, труд – прежде всего),

- способность ставить перед сотрудниками СБ задачи по сбору информации (в добро желательной манере, критика в их адрес – слабость аналитика), умение обучать сотрудников СБ и побуждать их к совершенствованию навыков подготовки аналитических материалов, чтобы добиться от сотрудников СБ такой проработки первичных документов, которая позволит аналитику экономить время и использовать его для обучения персонала СБ азам аналитической работы.

Практика показывает, что в частных структурах безопасности аналитическую работу в настоящее время ведут лица, имеющие прошлый опыт работы в государственных силовых ведомствах. У них еще есть (при заинтересованном подходе предпринимателей) срок подготовить себе профессиональную замену. Нужно правильно наладить работу внутри СБ: постоянный обмен опытом, профессиональную учебу, оказание помощи начинающим аналитикам и т.д.

Аналитик СБ должен хорошо ориентироваться:

- в вопросах внешней и внутренней политики,

- в проблемах рыночной экономики, финансов, маркетинга,

- в процессах финансового и других видах мошенничества,

- в окружающей криминальной и террористической среде,

- в поисковых системах Интернета,

- в местных и иностранных СМИ,

- в специальной тематической литературе,

- в грамматике и стилистике языка,

- в мире разнообразной справочной и словарной литературы,

- иметь представление обо всем, но досконально знать одну – две темы и во многом другом.

Аналитик СБ, как правило, должен владеть иностранным языком. В СБ, которые имеют зарубежные филиалы, это является обязательным условием для карьеры аналитика и т.д. Обязанности и права аналитика СБ.

Аналитик обязан:

- быть всегда в хорошей физической и интеллектуальной форме (заказ на написание документа обычно поступает неожиданно, его подготовка иногда затягивается на неопределенный срок – день, ночь, суббота, воскресенье и т.д.),

- быть всегда в курсе политики руководства (предвидеть проблемы, которые могут возникнуть у руководства и которые могут потребовать их срочного анализа),

- иметь под рукой определенный информационный задел для начала составления аналитического документа, до поступления заказанных конфиденциальных сведений,

- досконально знать пути поиска и сбора необходимой информации в Интернете,

- уметь видеть за частоколом фактов главную цель и логическим путем шаг за шагом идти к ней,

- вовремя заметить ошибочный путь и вернуться на правильную дорогу (свет в темной комнате),

- обладать интуицией (предвидением), она может заменить недостающие факты, и особенно важна при выводах,

- иметь в запасе и постоянно пополнять различные вставки – шаблоны (нужны при срочном написании документов),

- писать грамотно, понятно, по – возможности, кратко,

- избегать внесения в аналитический документ, околонаучных терминов, высокого стиля, набивших оскомину словесных штампов и т.д.,

- подстраиваться под стиль письма и разумения руководства (это не подхалимство, а рабочий момент аналитики, помогающий избежать последующих ненужных согласований и недоразумений в понимании смысла подготовленного документа),

- не паниковать в форс-мажорных обстоятельствах – отсутствие уверенности может свести к нулю все усилия растерянного аналитика, поскольку его мозг будет занят мыслями о подготовке документа к указанному сроку и в противном случае о грядущем служебном наказании,

- объяснить руководству внятно, доходчиво и уверенно непонятые тому части подготовленного аналитического документа,

- при подаче аналитического документа на подпись иметь под рукой основные

материалы, которые использовались при его подготовке,

- не спорить с руководством, если делать какие – то замечания по ходу неудовлетворительного для аналитика рассмотрения документа, то очень доказательно,

- светиться уверенностью в значимости представленного документа.

Аналитик не должен:

- писать заумно (показывать свою ученость), документы, написанные заумно, как правило, читаются с трудом, до главной мысли приходиться пробираться через чащу абсолютно ненужных и часто непонятных потребителю терминов,

- стремиться объять «необъятное» (у начинающего аналитика всегда под рукой «много важной информации», которую хотелось бы вставить в документ),

- растекаться мыслью по древу: в аналитике краткость – сестра таланта,

- вставлять в аналитический материал не проверенные, сомнительные факты без их собственного комментария,

- давать волю субъективным суждениям, не подтверждающимися объективными фактами,

- не быть категоричным в суждениях – освещение реальных событий и прогнозирование требуют гибкости в суждениях, поскольку природа вещей многогранна,

- делать выводы, не вытекающие из основного содержания аналитического документа, и на далекую перспективу,

- «обижаться» на внесенные руководством коррективы – оно обладает большим объемом информации, более широким видением проблемы в общей ситуации и реальном отрезке времени.

Аналитик имеет право:

- быть допущенным к основным конфиденциальным документам, в части его касающейся, и рассчитывать на помощь в подготовке дополнительных информационных материалов,

- при необходимости получать от руководства рекомендации по составлению аналитического документа, советоваться с руководством соответствующих отделов во время написания аналитического документа,

- свободно (в разумных пределах) распоряжаться своим рабочим графиком в рамках реального времени, отпущенного на написание аналитического документа.

Советы по работе с начинающими аналитиками:

- вспомните, как вы начинали свою работу,

- вспомните все то, что вы хотели получить и не получили от своего наставника,

- не повторяйте ошибок своих учителей, будьте вежливы и терпеливы с молодыми сотрудниками,

- не раздражайтесь и в состоянии раздражения не делайте за них их же работу,

- дайте понять, что в отделе все равны, и каждый обязан честно и качественно делать свою работу,

- хороший будущий сотрудник надоедает постоянными вопросами, если они по – делу, не горячитесь, и отвечайте на них спокойно,

- на первых порах совместно разбирайте написанное, не стесняясь, указывайте на ошибки,

- давая задание, обязательно проверьте его исполнение,

- будьте учителем, а не ментором,

- остужайте молодые, талантливые, горячие головы, пресекайте бахвальство, шапкозакидательство,

- будьте скупы на похвалу, но за дело похвалите,

- не демонстрируйте молодым свою опытность, у них не было времени её приобрести.

1.2. Специфика теоретического познания и его формы

Теоретический уровень научного познания характеризуется преобладанием рационального момента – понятий, теорий, законов и других форм мышления и «мыслительных операций». Живое созерцание, чувственное познание здесь не устраняется, а становится подчиненным (но очень важным) аспектом познавательного процесса. Теоретическое познание отражает явления и процессы со стороны их универсальных внутренних связей и закономерностей, постигаемых с помощью рациональной обработки данных эмпирического знания. Эта обработка осуществляется с помощью систем абстракций «высшего порядка» – таких как понятия, умозаключения, законы, категории, принципы и др.

На основе эмпирических данных здесь происходит мысленное объединение исследуемых объектов, постижение их сущности, законов их существования, составляющих основное содержание теорий – «квинтэссенции» знания на данном уровне. Важнейшая задача теоретического знания – достижение объективной истины во всей ее конкретности и полноте содержания. При этом особенно широко используются такие познавательные приемы и средства как абстрагирование – отвлечение от ряда свойств и отношений предметов, идеализация – процесс создания чисто мысленных предметов, синтез – объединение полученных в результате анализа элементов в систему, дедукция – движение познания от общего к частному, восхождение от абстрактного к конкретному и др. Присутствие в познании идеализации служит показателем развитости теоретического знания как набора определенных идеальных моделей.

Характерной чертой теоретического познания является его направленность на себя, внутринаучная рефлексия, т.е. исследование самого процесса познания, его форм, приемов, методов, понятийного аппарата и т.д. На основе теоретического объяснения и познанных законов осуществляется предсказание, научное предвидение будущего.

На теоретической стадии науки преобладающим (по сравнению с живым созерцанием) является рациональное познание, которое наиболее полно и адекватно выражено в мышлении. *Мышление* – осуществляющийся в ходе практики активный процесс обобщенного и опосредованного отражения действительности, обеспечивающий раскрытие на основе чувственных данных ее закономерных связей и их выражение в системе абстракций (понятий, категорий и др.). Человеческое мышление осуществляется в теснейшей связи с речью, а его результаты фиксируются в языке как определенной знаковой системе, которая может быть естественной или искусственной (язык математики, формальной логики, химические формулы и т.п.).

Говоря о важнейшем значении мышления для научного познания, М. Борн подчеркивал, что «человеческий ум может проникать в тайны природы с помощью мышления вследствие гармонии между законами мышления и законами природы». Отсутствие такой гармонии, расхождение законов мышления с законами бытия закрывает путь к истине, ведет к заблуждению.

Мышление человека – не природное его свойство, а выработанная в ходе истории функция социального субъекта, общества в процессе своей предметной деятельности и общения, идеальная их форма. Поэтому мышление, его формы, принципы, категории, законы и их последовательность внутренне связаны с историей социальной жизни, обусловлены развитием труда, практики. Именно уровень и структура последней обусловливают в конечном итоге способ мышления той или иной эпохи, своеобразие логических «фигур» и связей на каждом из ее этапов. Вместе с развитием практики, ее усложнением и внутренней дифференциацией изменяется и мышление, проходя определенные уровни (этапы, состояния и т.п.). Исходя их древней философской традиции, восходящей к античности, следует выделить два основных уровня мышления – рассудок и разум.

Рассудок – исходный уровень мышления, на котором оперирование абстракциями происходит в пределах неизменной схемы, заданного шаблона, жесткого стандарта. Это способность последовательно и ясно рассуждать, правильно строить свои мысли, четко классифицировать, строго систематизировать факты. Здесь сознательно отвлекаются от развития, взаимосвязи вещей и выражающих их понятий, рассматривая их как нечто устойчивое, неизменное. Главная функция рассудка – расчленение и исчисление. Мышление в целом невозможно без рассудка, он необходим всегда, но его абсолютизация неизбежно ведет к метафизике. Рассудок – это обыденное повседневное житейское мышление или то, что часто называют здравым смыслом. Логика рассудка – формальная логика, которая изучает структуру высказываний и доказательств, обращая основное внимание на форму «готового» знания, а не на его содержание.

Разум – (диалектическое мышление) – высший уровень рационального познания, для которого прежде всего характерны творческое оперирование абстракциями и сознательное исследование их собственной природы (саморефлексия). Только на этом своем уровне мышление может постигнуть сущность вещей, их законы и противоречия, адекватно выразить логику вещей в логике понятий. Последние как и сами вещи

берутся в их взаимосвязи, развитии, всесторонне и конкретно. Главная задача разума – объединение многообразного вплоть до синтеза противоположностей и выявления коренных причин и движущих сил изучаемых явлений. Логика разума – диалектика, представленная как учение о формировании и развитии знаний в единстве их содержания и формы.

Процесс развития мышления включает в себя взаимосвязь и взаимопереход рассудка и разума. Наиболее характерной формой перехода первого во второй является выход за пределы сложившейся готовой системы знания, на основе выдвижения новых – диалектических по своей сути – фундаментальных идей. Переход разума в рассудок связан прежде всего с процедурой формализации и перевода в относительно устойчивое состояние тех систем знания, которые были получены на основе разума (диалектического мышления).

Формы мышления (логические формы) – способы отражения действительности посредством взаимосвязанных абстракций, среди которых исходными являются понятия, суждения и умозаключения. На их основе строятся более сложные формы рационального познания, такие, как гипотеза, теория и другие, которые будут рассмотрены ниже.

Понятие – форма мышления, отражающая общие закономерные связи, существенные стороны, признаки явлений, которые закрепляются в их определениях (дефинициях). Например, в определении «человек есть животное, делающее орудия труда» выражен такой существенный признак человека, который отличает его от всех других представителей животного мира, выступает фундаментальным законом существования и развития человека как родового существа. Понятия должны быть гибки и подвижны, взаимосвязаны, едины в противоположностях, чтобы верно отразить реальную диалектику (развитие) объективного мира. Наиболее общие понятия – это философские категории (качество, количество, материя, противоречие и др.). Понятия выражаются в языковой форме – в виде отдельных слов («атом», «водород» и др.) или в виде словосочетаний, обозначающих классы объектов («экономические отношения», «элементарные частицы» и др.).

Суждение – форма мышления, отражающая вещи, явления, процессы действительности, их свойства, связи и отношения. Это мысленное отражение, обычно выражаемое повествовательным предложением, может быть либо истинным («Париж стоит на Сене»), либо ложным («Ростов – столица России»). В форме суждения отражаются любые свойства и признаки предмета, а не только существенные и общие (как в понятии). Например, в суждении «золото имеет желтый цвет» отражается не существенный, а второстепенный признак золота.

Понятия и суждения выступают «кирпичиками» для построения умозаключений, которые представляют собой моменты движения от одних понятий к другим, выражают процесс получения новых результатов в познании. *Умозаключение* – форма мышления, посредством которой из ранее установленного знания (обычно из одного или нескольких суждений) выводится новое знание (также обычно в виде суждения). Классический пример умозаключения:

1. Все люди смертны (посылка).

2. Сократ – человек (обосновывающее знание).

3. Следовательно, Сократ смертен (выводное знание, называемое заключением или следствием).

Важными условиями достижения истинного выводного знания являются не только истинность посылок (аргументов, оснований), но и соблюдение правил вывода, недопущение нарушений законов и принципов логики – не только формальной, но и диалектической. Наиболее общим делением умозаключений, является их деление на два взаимосвязанных вида: индуктивное движение мысли от единичного, частного к общему, от менее общего к более общему, и дедуктивное, где имеет место обратный процесс (как в приведенном примере).

Следует иметь в виду, что рациональное (мышление) взаимосвязано не только с чувственным, но и с другими – внерациональными – формами познания. Большое значение в процессе познания имеют такие факторы, как воображение, фантазия, эмоции и др. Среди них особенно важную роль играет интуиция (внезапное озарение) – способность прямого, непосредственного постижения истины без предварительных логических рассуждений и без доказательств. В истории философии на важную роль интуиции (хотя и по-разному понимаемой) в процессе познания указывали многие мыслители. Так, Декарт считал, что для реализации правил своего рационалистического метода необходима интуиция, с помощью которой усматриваются первые начала (принципы), и дедукция, позволяющая получить следствия из этих начал.

История познания показывает, что новые идеи, коренным образом меняющие старые представления, часто возникают не в результате строго логических рассуждений или как простое обобщение. Они являются как бы скачком в познании объекта, перерывом непрерывности в развитии мышления. Для интуитивного постижения действительности характерна свернутость рассуждений, осознание не всего их хода, а отдельного наиболее важного звена, в частности, окончательных выводов.

Полное логическое и опытное обоснование этих выводов им находят позднее, когда они уже были сформулированы и вошли в ткань науки. Как писал известный французский физик Луи де Бройль, «человеческая наука, по существу рациональная в своих основах и по своим методам, может осуществлять свои наиболее замечательные завоевания лишь путем опасных внезапных скачков ума, когда проявляются способности, освобожденные от тяжелых оков строгого рассуждения, которые называют воображением, интуицией, остроумием». Крупнейший математик А. Пуанкаре говорил о том, что в науке нельзя все доказать и нельзя все определить, а поэтому приходится всегда «делать заимствования у интуиции». Действительно, интуиция требует напряжения всех познавательных способностей человека, в нее вкладывается весь опыт предшествующего социокультурного и индивидуального развития человека – его чувственно-эмоциональной сферы (чувственная интуиция) или его разума, мышления (интеллектуальная интуиция). Многие великие творцы науки подчеркивали, что нельзя недооценивать важную роль воображения, фантазии и интуиции в научном исследовании. Однако чтобы не зайти в тупик, интуитивный момент следует соединять с дискурсивным (логическим, понятийным, опосредованным), имея в виду, что это два необходимо связанных момента единого познавательного процесса.

Познание как единство чувственного и рационального, эмпирического и теоретического, рассудка и разума, интуитивного и дискурсивного тесно связано с

пониманием. Последнее не сводится только к тому, чтобы изучаемый объект выразить в логике понятий. Понимание – это проникновение в смысл чего-либо (текста, феноменов культуры и т.п.), постижение посредством диалога чужой субъективности, другой личности.

Рассматривая теоретическое познание как высшую и наиболее развитую его форму, следует определить его структурные компоненты. К числу основных из них относятся проблема, гипотеза и теория, выступающие вместе с тем как формы, «узловые моменты» построения и развития знания на теоретическом его уровне.

Проблема – форма теоретического знания, содержанием которой является то, что еще не познано человеком, но что нужно познать. Иначе говоря, это знание о незнании, вопрос, возникший в ходе познания и требующий ответа. Проблема не есть застывшая форма знания, а процесс, включающий два основных момента (этапа движения познания) - ее постановку и решение. Правильное выведение проблемного знания из предшествующих фактов и обобщений, умение верно поставить проблему – необходимая предпосылка ее успешного решения. Формулировка проблемы часто более существенна, чем ее разрешение, которое может быть делом лишь математического или экспериментального искусства. Постановка новых вопросов, развитие новых возможностей, рассмотрение старых проблем под новым углом зрения требуют творческого воображения и отражают действительный успех в науке.

В. Гейзенберг отмечал, что при постановке и решении научных проблем необходимо следующее: а) определенная система понятий, с помощью которых исследователь будет фиксировать те или иные феномены; б) система методов, избираемая с учетом целей исследования и характера решаемых проблем; в) опора на научные традиции, поскольку, по мнению Гейзенберга, «в деле выбора проблемы традиция, ход исторического развития играют существенную роль», хотя, конечно, определенное значение имеют интересы и наклонности самого ученого. Как считает К. Поппер, наука начинает не с наблюдений, а именно с проблем, и ее развитие есть переход от одних проблем к другим – от менее глубоких к более глубоким. Проблемы возникают, по его мнению, либо как следствие противоречия в отдельной теории, либо при столкновении двух различных теорий, либо в результате столкновения теории с наблюдениями. Тем самым научная проблема выражается в наличии противоречивой ситуации (выступающей в виде противоположных позиций), которая требует соответствующего разрешения. Определяющее влияние на способ постановки и решения проблемы имеют, во-первых, характер мышления той эпохи, в которую формулируется проблема, и, во-вторых, уровень знания о тех объектах, которых касается возникшая проблема. Каждой исторической эпохе свойственны свои характерные формы проблемных ситуаций.

Научные проблемы следует отличать от ненаучных (псевдопроблем), например, проблема создания вечного двигателя. Решение какой-либо конкретной проблемы есть существенный момент развития знания, в ходе которого возникают новые проблемы, а также выдвигаются те или иные концептуальные идеи, в том числе и гипотезы. Наряду с теоретическими существуют и практические проблемы.

Гипотеза – форма теоретического знания, содержащая предположение, сформулированное на основе ряда фактов, истинное значение которого неопределенно и нуждается в доказательстве. Гипотетическое знание носит вероятный, а не достоверный характер и требует проверки, обоснования. В ходе

доказательства выдвинутых гипотез одни из них становятся истинной теорией, другие видоизменяются, уточняются и конкретизируются, третьи отбрасываются, превращаются в заблуждения, если проверка дает отрицательный результат. Выдвижение новой гипотезы, как правило, опирается на результаты проверки старой, даже в том случае, если эти результаты были отрицательными. Выдающиеся ученые хорошо понимали важную роль гипотезы для научного познания. Гипотеза может существовать лишь до тех пор, пока не противоречит достоверным фактам опыта, в противном случае она становится просто фикцией. Она проверяется (верифицируется) соответствующими опытными фактами (в особенности экспериментом), получая характер истины. Гипотеза является плодотворной, если может привести к новым знаниям и новым методам познания, к объяснению широкого круга явлений.

Гипотеза как метод развития научно-теоретического знания в своем применении проходит следующие основные этапы.

1. Попытка объяснить изучаемое явление на основе известных фактов и уже имеющихся в науке законов и теорий. Если такая попытка не удается, то делается дальнейший шаг.

2. Выдвижение догадки, предположения о причинах и закономерностях данного явления, его свойств, связей и отношений, о его возникновении и развитии и т.п. На этом этапе познания выдвинутое положение представляет собой вероятное знание, еще не доказанное логически и не настолько подтвержденное опытом, чтобы считаться достоверным. Чаще всего выдвигается несколько предположений для объяснения одного и того же явления.

3. Оценка основательности, эффективности выдвинутых предположений и отбор из их множества наиболее вероятного на основе указанных свыше условий обоснованности гипотезы.

4. Развертывание выдвинутого предположения в целостную систему знания и дедуктивное выведение из него следствий с целью их последующей эмпирической проверки.

5. Опытная, экспериментальная проверка выдвинутых из гипотезы следствий. В результате этой проверки гипотеза либо «переходит в ранг» научной теории, или опровергается, «сходит с научной сцены». Однако следует иметь в виду, что эмпирическое подтверждение следствий из гипотезы не гарантирует в полной мере ее истинности, а опровержение одного из следствий не свидетельствует однозначно о ее ложности в целом. Эта ситуация особенно характерна для научных революций, когда происходит коренная ломка фундаментальных концепций и методов и возникают принципиально новые (и зачастую «сумасшедшие», по словам Н. Бора) идеи.

Таким образом, решающей проверкой истинности гипотезы является, в конечном счете, практика во всех своих формах, но определенную (вспомогательную) роль в доказательстве или опровержении гипотетического знания играет и логический (теоретический) критерий истины. Проверенная и доказанная гипотеза переходит в разряд достоверных истин, становится научной теорией.

Теория – наиболее развития форма научного знания, дающая целостное отображение закономерных и существенных связей определенной области действительности. Примерами этой формы знания являются классическая механика Ньютона,

эволюционная теория Ч. Дарвина, теория относительности А. Эйнштейна, теория самоорганизующихся целостных систем (синергетика) и др.

А. Эйнштейн считал, что любая научная теория должна отвечать следующим критериям: а) не противоречить данным опыта, фактам; б) быть проверяемой на имеющемся опытном материале; в) отличаться «естественностью», т.е. «логической простотой» предпосылок (основных понятий и основных соотношений между ними; г) содержать наиболее определенные утверждения: это означает, что из двух теорий с одинаково «простыми» основными положениями следует предпочесть ту, которая сильнее ограничивает возможные априорные качества систем; д) не являться логически произвольно выбранной среди приблизительно равноценных и аналогично построенных теорий (в таком случае она представляется наиболее ценной); е) отличаться изяществом и красотой, гармоничностью; ж) характеризоваться многообразием предметов, которые она связывает в целостную систему абстракций; з) иметь широкую область своего применения с учетом того, что в рамках применимости ее основных понятий она никогда не будет опровергнута; и) указывать путь создания новой, более общей теории, в рамках которой она сама остается предельным случаем.

Любая теоретическая система должна удовлетворять двум основным требованиям: а) непротиворечивости (т.е. не нарушать соответствующий закон формальной логики) и фальсифицируемое – опровержимости, б) опытной экспериментальной проверяемости. Истинная теория должна, во-первых, соответствовать всем (а не некоторым) реальным фактам, а, во-вторых, следствия теории должны удовлетворять требованиям практики.

1.3. Аналитика - знание - информация

Современный мир каждодневно обогащается новыми знаниями, получая их из научных открытий и научных трудов, популярной научной литературы, беллетристики, произведений художников, СМИ и т.д. Философский словарь определяет знание как «продукт общественно-трудовой и мыслительной деятельности людей, представляющий идеальное воспроизведение в языковой форме объективных, закономерных связей практически преобразуемого мира». Методы познания, как таковые, применяются нами бессознательно везде и всегда, с самой первой минуты нашего рождения. Мы мыслим абстрактными категориями, используем законы логики, с их помощью ежесекундно изучаем окружающий нас мир. Но, как известный мольеровский герой не знал о том, что всю жизнь говорит прозой, так и мы не задумываемся о том, что всю свою сознательную жизнь живем и действуем по данным нам природой законам мышления. Человеческое сознание не в состоянии охватить сразу все накопленное знание. Поэтому каждый человек получает необходимые ему сведения частями, которые складываются в слова, предложения, тексты, символы, цифры, формулы, уравнения и т.д. В структурированном виде, все это является знанием – информацией о каком-либо событии, факте или явлении. В соответствии с Законом РФ «Об информации, информатизации и защите информации»: «Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». Накопленная человечеством информация не может

оставаться «мертвой». Она объективно востребована для извлечения полезного знания из прошлого опыта. Это полезное знание используется для обучения современного поколения. Современное поколение, основываясь на прошлом знании, добывает новое знание и т.д. Угроза существования «мертвой информации», (разрыв между уже добытым человечеством знанием и низкой степенью его востребованности из-за объективно существующих проблем: трудно доступности или дороговизны его получения) была ликвидирована созданием всемирной информационной системы Интернета, которая приобщила к общемировым информационным источникам миллиарды людей. Предвосхищая современный информационный бум, В.И. Вернадский писал: «...Мощь его (человечества) не связана с его материей, но с его мозгом, с его разумом и направленным этим разумом его трудом... И перед ним его мыслью и трудом, ставится вопрос о перестройке биосферы в интересах свободно мыслящего человечества как единого целого».

Сегодня информация становится «локомотивом» процесса мировой глобализации, предвестником общемировой «стандартизации» человеческого сообщества. Одновременно с этим, специфические свойства информации (её негативное влияние на человеческий мозг при целенаправленном воздействии, пропагандистском и техническом её оснащении) превращают информацию в грозное оружие 21-ого века, наряду с другими мощнейшими видами вооружения, изобретенными человечеством для своего уничтожения.

Борьба между позитивным и негативным воздействием информации на умы людей является объективной реальностью, в горниле которой в ближайшей перспективе и будет выковываться новый этап эволюции человечества.

Знание – информация делится на:

- *эмпирическое знание* (экспериментальное), полученное в своем «первозданном» виде в процессе изучения учеными законов природы и эволюции человечества в таких науках как химия, физика, археология, ботаника, зоология, палеонтология и т.д.

- *логическое знание* (аналитическое) математика, астрономия, молекулярная физика и т.д. Это расширенное знание, углубленное познавательным процессом человека. Здесь большую роль играет научное предвидение, интуиция.

- *художественное знание* – "выданное" художником, музыкантом, литератором, отображающими объективную реальность художественными методами.

- *обыденное знание* – традиции, нормы и правила поведения, национальные особенности и т.д.

- *оперативное знание* – информация, необходимая для повседневной ориентации человеческого сообщества в политических, военных, социально – экономических проблемах, вопросах научно технического развития, предвидении социальных, техногенных и природных катаклизмов и т.д.

- «протознание» – архивное знание.

Вместе с тем, все эти деления условны, поскольку человеческое знание – это единый процесс познания окружающего нас мира, где один вид знания перетекает в другой, где одно знание устаревает и его сменяет новое. Исток этого процесса находится в

повседневной человеческой практике, а сама река знания формируются в мозге человека и, расширяясь, несется через различные пороги к своему устью – познанию абсолютной истины. То есть, проще говоря, к тому, чтобы узнать, кто мы есть, зачем пришли в этот мир, что мы в нем и с ним обязаны делать?

Оперативная информация структур безопасности (закрытая и открытая), добываемая (легальным путем и специфическими средствами) – это только частица общечеловеческого оперативного знания. Она необходима для обеспечения безопасности деятельности предпринимательских структур и обладает только ей присущими свойствами, обусловленными объективными законами развития рыночной экономики и системы её охраны. Основная цель получения такой оперативной информации – выживание предпринимательской структуры в конкурентной рыночной среде, которую в основном формируют государственные органы, конкуренты-предприниматели, криминальные структуры. Экономические условия рынка регулируются законами товарного производства, но опутаны многочисленными сетями государственных законов, правилами рыночной конкуренции, порождающими криминал. Жить, действовать разумно в этих жестких рамках и выжить – можно только при условии хорошей информированности о планах государственных чиновников, конкурентов и криминальных авторитетов.

Простой пример, предприниматель и его служба безопасности тратят много времени и финансовых средств, чтобы наладить контакты в госструктурах, курирующих бизнес. Они нашли, в конце концов, подходы к нужным чиновникам, но тут внезапно узнают о реорганизации правительства... и выясняется, что все их усилия были напрасными. Нужно начинать все заново. Для того чтобы предвидеть все нюансы развития кризисной ситуации, необходима информация и, прежде всего, информация: закрытая, конфиденциальная, упреждающая, прогнозирующая. Остальное – дело аналитика, который на её основе выдает то или иное решение проблемы. Нехватку информации аналитик восполняет своей интеллектуальной способностью к анализу.

Сегодняшний аналитик – наемный работник умственного труда, который продает свой товар интеллектуальную способность в её различных проявлениях предпринимателю, путем предоставления последнему аналитически выверенного нового выводного знания, на базе которого тот должен в принципе строить тактику и стратегию развития своего дела (бизнеса).

Подготовленный аналитиком новый документ тут же отчуждается от своего создателя, поскольку в него вносятся те или иные поправки и новое выводное знание становится коллективным творчеством службы безопасности и руководства фирмы, предприятия, банка и т.д., то есть интеллектуальной коллективной собственностью.

Важно отметить, что подготовленный специалистом аналитический документ (при всей его объективности) может быть принят или отвергнут предпринимателем, имеющим свою точку зрения (при наличии более глубокой информации, недоступной по различным причинам аналитику) на существующую проблему. В этих противоречиях между аналитиком и предпринимателем (если они носят рабочий и объективный характер) обычно рождается предпринимательская истина. Таким образом, аналитический материал только тогда становится аналитическим документом, когда он принят предпринимателем к действию, поскольку лежащие в нем выводы отвечают субъективно понятой последним объективной реальности, сложившейся на рынке к данному моменту.

1.4. Процессы анализа и синтеза

Начнем с небольшого отступления. Скульптору предложили изваять женскую фигуру и для этого привезли огромную каменную глыбу. Скульптор внимательно осмотрел камень, ощупал руками его фактуру и задумался несколько минут, мысленно представив себе, что может получиться из этой глыбы. Затем, по только автору известным приметам, начал отсекать кусок за куском от глыбы. Постепенно глыба стала принимать грубые очертания женской фигуры. Он трудился много дней. И вот, наконец, скульптор последним ударом молотка по резцу закончил работу и перед зрителями в глубине каменной глыбы открылся силуэт прекрасного женского лица.

Так человек, при помощи мысли и труда, в результате творческого процесса, из многофактурного и одновременно монолитного валуна, учитывая при работе свойства и качества камня, его внутреннюю структуру, получил спрятанный в ней природой шедевр. Также работает и аналитик, который из «информационной глыбы» (объём информации для аналитической обработки) создает свой аналитический шедевр. В мыслительных операциях анализ выступает как логические приемы мышления, совершающиеся при помощи абстрактных понятий и тесно связанные с другими мыслительными операциям: абстракцией, обобщением и т.д. Анализ и синтез играют важную роль в познавательном процессе и осуществляются на всех его этапах. Большую роль в познании играют также воображение, творческая фантазия, интуиция. Они позволяют аналитику, оживить свою мыслительную работу, увидеть тот или иной факт с такой стороны, которая не просматривается строго логически. Все это объединяется в понятии «творческий процесс». Естественно, творческий процесс требует мобилизации максимума активности, знаний и способностей аналитика. Такая мобилизация находит свое выражение в волевом напряжении и эмоциональном состоянии – творческом озарении, интуиции – способности непосредственного постижения истины без предварительного логического рассуждения. Наверное, этот волнующий душу момент и является по-настоящему, началом и венцом практического процесса аналитического мышления.

Есть несколько смыслов, в которых употребляются термины «анализ» и «синтез». Во-первых, это анализ и синтез как характеристики строения доказательства в математике. В этом смысле говорят об аналитическом и синтетическом методах и т.п. Во-вторых, анализ и синтез в смысле кантовского различения «аналитических» и «синтетических» суждений, которое фактически означало отличение способа получения знаний путем чисто логической обработки данного опыта («аналитическое») от способа получения знаний путем обращения к содержанию, путем привлечения к исходному знанию каких-то иных данных опыта («синтетическое»). Но анализ и синтез с самого начала интересуют нас как движение в определенном содержании, отличное от получения знания путем формального вывода. Поэтому различение «аналитических» и «синтетических» суждений здесь неприменимо, ибо с этой точки зрения каждый момент движения мысли был бы синтетичен и, следовательно, в нем нельзя было бы увидеть никаких различий.

Наконец, чаще всего термины «анализ» и «синтез» употребляются применительно ко всему мышлению в целом, к исследованию вообще. Познавая предметы, мы определенным образом их расчленяем, выделяем в них и рассматриваем отдельно те или иные их стороны, свойства, связи, то есть, производим «анализ». Мышление

вообще есть отражение посредством абстракций. С другой стороны, всякое мышление есть установление каких-то отношений между зафиксированными в мысли предметами или их сторонами, то есть «синтез».

Анализ (от греч. análysis – разложение, расчленение), процедура мысленного, а часто также и реального расчленения предмета (явления, процесса), свойства предмета (предметов) или отношения между предметами на части (признаки, свойства, отношения); процедурой, обратной анализу, является синтез, с которым анализ часто сочетается в практической или познавательной деятельности. Аналитические методы настолько распространены в науке, что термин «анализ» часто служит синонимом исследования вообще как в естественных, так и в общественных науках (количественный и качественный анализ в химии, диагностический анализ в медицине, разложение сложных движений на составляющие в механике, функциональный анализ в социологии и т. д.).

Процедуры анализа входят органической составной частью во всякое научное исследование и обычно образуют его первую стадию, когда исследователь переходит от нерасчленённого описания изучаемого объекта к выявлению его строения, состава, а также его свойств, признаков. Но и на других ступенях познания анализ сохраняет своё значение, хотя здесь он выступает уже в единстве с другими процедурами исследования. Аналитические процедуры являются одними из главных не только в научном мышлении, но и во всякой деятельности, поскольку она связана с решением познавательных задач. Как познавательный процесс анализ изучается психологией, рассматривающей его как психический процесс, который осуществляется на различных уровнях отражения действительности в мозгу человека и животных, а также теорией познания и методологией науки, которые рассматривают анализ, прежде всего, как один из приёмов (методов) получения новых познавательных результатов.

Анализ присутствует уже на чувственной ступени познания и, в частности, включается в процессы ощущения и восприятия; в своих более простых формах он присущ даже животным. Однако аналитико-синтетическая деятельность даже высших животных непосредственно включена в их внешние действия. У человека к чувственно-наглядным формам анализа присоединяется высшая форма анализа – мыслительный, или абстрактно-логический, анализ. Эта форма анализа возникла вместе с навыками материально-практического расчленения предметов в процессе труда; по мере усложнения последнего человек овладевал способностью предварять материально-практический анализ мыслительным.

Развитие производственной деятельности, мышления и языка, приёмов научного исследования и доказательства привело к появлению разных форм мыслительного анализа, в частности расчленения предметов на неотделимые от них признаки, свойства, отношения. В отличие от чувственно-наглядного, мыслительный анализ совершается с помощью понятий и суждений, выражаемых в естественных или искусственных языках (знаковых системах науки). С другой стороны, и сам анализ, вместе с другими приёмами, служит средством формирования понятий о действительности.

Существует несколько видов анализа как приёма научного мышления. Одним из них является мысленное (а часто, например, в эксперименте, и реальное) расчленение целого на части. Такой анализ, выявляющий строение (структуру) целого, предполагает не только фиксацию частей, из которых состоит целое, но и

установление отношений между частями. При этом особое значение имеет случай, когда анализируемый предмет рассматривается как представитель некоторого класса предметов: здесь анализ служит установлению одинаковой (с точки зрения некоторых отношений) структуры предметов класса, что позволяет переносить знание, полученное при изучении одних предметов, на другие. Другим видом анализа является анализ общих свойств предметов и отношений между предметами, когда свойство или отношение расчленяется на составляющие свойства или отношения; одни из них подвергаются дальнейшему анализу, а от других отвлекаются; на следующем этапе анализа может подвергнуться то, от чего ранее отвлеклись, и т.д. В результате анализа общих свойств и отношений понятия о них сводятся к более общим и простым понятиям. Видом анализ является также разделение классов (множеств) предметов на подклассы – непересекающиеся подмножества данного множества. Такого рода анализ называют классификацией. Все эти и другие виды анализа применяются как при получении нового знания, так и при систематическом изложении уже имеющихся научных результатов. Анализ широко используют также в педагогическом процессе.

Описанному смыслу понятия анализа родственно более специальное понятие формально-логического (логического) анализ. Логический анализ – это уточнение логической формы (строения, структуры) рассуждения, осуществляемое средствами современной формальной логики. Такое уточнение может касаться как рассуждений (логических выводов, доказательств, умозаключений и т. п.) и их составных частей (понятий, терминов, предложений), так и отдельных областей знания. Наиболее развитой формой логического анализа содержательных областей знания, содержательных понятий и способов рассуждения является построение формальных систем, интерпретируемых на этих областях или с помощью данных понятий, – формализованных языков. Логический анализ – один из основных познавательных приёмов науки, значение которого особенно возросло благодаря развитию математической логики, кибернетики, семиотики и разработке информационно-логических систем.

В ином смысле понимается анализ в истории математики. Здесь анализ – это рассуждение, идущее от того, что подлежит доказательству (от неустановленного, неизвестного), к тому, что уже доказано (установлено ранее, известно); под синтезом же понимается рассуждение, идущее в обратном направлении. Анализ в этом смысле является средством выявления идеи доказательства, но в большинстве случаев сам по себе доказательством ещё не является. Синтез же, опираясь на данные, найденные в анализе, показывает, как из ранее установленных утверждений вытекает доказываемое, даёт доказательство теоремы или решение задачи.

Собственно анализ и синтез есть мысленное расчленение и соединение предметов в указанном выше смысле. Однако необходимо при этом учесть, что исторически содержание этого процесса логической деятельности формируется впервые в предметно-вещественной деятельности человека (то есть отнюдь не в созерцании) и только впоследствии распространяется на предметы, связанные отношением «целое – часть», независимо от практики человека. На этом основаны как связь, так и различие вещественной и логической деятельности.

Хотя процесс логического анализа и синтеза и возникает из практически-чувственной деятельности человека, но, раз возникнув, обладает своими собственными законами.

Это видно уже из того, что практическое расчленение и воссоединение предмета исключают друг друга (расчленение предмета не дает его соединения), тогда как в применении к логическому процессу мы будем говорить об анализе посредством синтеза, и наоборот.

«Часть» – внешне обособленный предмет, входящий в состав другого предмета («целого») и выполняющий в нем определенную роль. «Целое» – предмет, состоящий из различных частей и обладающий в силу этого определенными свойствами, которых нет у отдельных частей и которые присущи лишь их координации. «Суммативных» целых (то есть таких, которые целиком сводятся к свойствам своих отдельных частей) вообще не бывает. С другой стороны, целое не существует как особый, самостоятельный предмет наряду со своими частями. Оно отличается от своих частей лишь так, как координация отличается от координированных в ней элементов. Задача процесса отражения здесь заключается в том, чтобы зафиксировать части как различные и их отношение как координацию, а целое – как координированную сумму частей, выполняющих в нем в силу своих различий различную роль. Например, исследование какого-либо химического соединения должно раскрыть в нем его части и дать формулу его состава, объяснить его свойства как целого. Построение теории о какой-то предметной области предполагает наличие и аналитического и синтетического знания о каждом предмете этой области, объективно состоящем из частей: особого знания об отдельных предметах связи и знания о свойствах связи предметов, заключающего в себе результат переработки воедино отдельных знаний.

Заметим, что синтетическое знание никогда не является простой механической суммой знаний о частях; оно представляет собой новое знание.

Структурно единство анализа и синтеза означает как взаимозависимость знаний (аналитического и синтетического) или задач исследования, так и характеристику способа осуществления каждой из них в отдельности. Уже элементарный процесс отражения простейшей координации и ее различных элементов есть одновременно и анализ и синтез в смысле получения аналитического знания посредством синтеза и синтетического знания посредством анализа.

Анализ есть вычленение отличных друг от друга частей и изолированное фиксирование их свойств в знании. Но «часть» – не просто пространственно отграниченный предмет с какими-то его свойствами, которые играют роль в его координации с другими частями целого. И если при анализе части интересуют исследователя в их отличии друг от друга, то имеются в виду не различия их и сходства, выделяемые сравнением и элементарным абстрагированием, а различия их места в связи. Анализ предмета осуществляется посредством синтеза частей.

Но, с другой стороны, такое синтетическое сопоставление предметов предполагает знание связи целого. Синтез есть выявление координации частей и определяемых ею свойств целого. Само целое есть особый, самостоятельный предмет, обладающий и рядом свойств, которые вовсе не вытекают из наличия в нем частей, и отражение его как такового в знании отнюдь не есть синтез. Задача заключается в том, чтобы выявить его свойства, обусловленные связью каких-то специфических необходимых частей. Не будучи расчленено на последние, целое вообще не выступает как специфическое целое. Жидкость, не содержащая кислород, не есть вода.

Целое или нельзя зафиксировать как отличное от других (например, воду в отличие от

сходных жидкостей вообще), или его нельзя объяснить в зафиксированных отличиях, не выделяя из него части и не рассматривая их последовательно. Лишь расчленяя целое на части и последовательно фиксируя их свойства, мы воспроизводим его как данное целое. Процесс анализа частей здесь дает синтез.

Таким образом, аналитическая и синтетическая задачи осуществляются каждая противоположно направленным в своих частях процессом. Это противоречивость самого процесса отражения. Лишь соединяя мысленно (или экспериментально), исследователь осознает части как части данного целого; лишь разлагая мысленно (или экспериментально), исследователь осознает целое как состоящее из специфических частей и обладающее вследствие этого специфическим свойством, отличающим его от других предметов.

Вывод. Методы научного познания неотделимы друг от друга и находятся в тесном единстве и взаимосвязи. Все научные методы можно условно разделить на две группы: общие и особенные. Общие методы позволяют связывать воедино все стороны процесса познания. К ним относят метод восхождения от абстрактного к конкретному, единство логического и исторического. Особенные методы касаются только одной стороны изучаемого предмета. Это наблюдение, эксперимент, анализ, синтез, индукция, дедукция, измерение, сравнение. Для безопасности наиболее важны методы анализа и синтеза.

Анализ – метод научного познания, в основу которого положена процедура мыслительного или реального расчленения предмета на составляющие части. Анализ обычно является начальной стадией любого исследования.

Синтез – метод научного исследования, основанный на соединении различных элементов предмета в единое целое, в систему. Синтез выступает не как метод конструирования целого, а как метод представления целого в форме единства знаний, полученных при анализе. При синтезе происходит не просто объединение, а обобщение аналитически выделенных и изученных особенностей объекта.

Необходимость анализа и синтеза в безопасности, например, в процессе принятия управленческих решений никогда не вызывала никаких сомнений. Практическое же его использование на макроуровне достаточно долго было ограничено лишь теми сферами, где чисто административные меры воздействия могли причинить слишком ощутимый и очевидный вред. Сейчас ситуация постепенно меняется к лучшему.

1.5. Информационная аналитика

Информационная аналитика в – это производство нового знания на основе переработки имеющейся информации в целях оптимизации принятия решений.

Универсальность социальной функции информационной аналитики и ее субстрата (информации) привели к эффекту мультидеятельностного генезиса аналитических служб (подразделений) во всех узлах информационной инфраструктуры, т.е. во всех сферах деятельности, где концентрировались, перерабатывались мощные информационные потоки в целях принятия социально значимых управленческих

решений. Именно поэтому информационно-аналитические службы (подразделения) стали создаваться в структуре органов федеральной и региональной власти, в министерствах и ведомствах, в органах СМИ, в сфере бизнеса, при политических партиях и движениях. Общей отличительной чертой данных служб являлась органическая включенность в соответствующие сферы деятельности, функциональный и организационно-деятельностный симбиоз с их социальными институтами и конкретными организациями. Аналитические службы в своих целях призваны осуществлять информационное сопровождение управления в соответствующих сферах.

Информационная аналитика не является всего лишь еще одной относительно новой организационной службой, ее сущностная, базовая функция принципиально отличается от тех задач, которые решают в информационном пространстве эти службы. Их задачи: количественные преобразования информации (информационное свертывание – библиографирование, аннотирование, реферирование; консолидация больших информационных массивов в виде баз и банков данных) и ее структурное упорядочение (систематизация, предметизация и т.п.). Информационная аналитика, используя все возможности, предоставляемые данными службами, активно оперируя их информационными продуктами и услугами, выполняет, прежде всего, задачу качественно-содержательного преобразования информации, функционально пересекаясь в этом плане с научной (производство нового знания) и управленческой (разработка вариантов решений, сценариев) деятельностью. Характер функционального взаимодействия в системе аналитика-наука-управление определяется спецификой аналитики. С наукой ее объединяет информационный способ познания и научного анализа реальности. Аналитика наиболее близка к гуманитарной науке, опирающейся на интерпретацию текстов, документов, сообщений о событиях и т.п., а также к тем разделам науки, видам научных задач, когда выводное знание получают не опытно-экспериментальным путем, а на основе анализа и интерпретации существующих теорий, описаний фактов, средствами информационного моделирования реальности.

Подобно исследователю такого профиля аналитик, опираясь на информационные модели (отпечатки в информационном пространстве событий, фактов, действий, идей, мнений, чувств людей, природных, социальных, политических, финансовых, экономических процессов и т.п.), выявляет в них объективные закономерности и тенденции, определяет движущие ими механизмы, причинно-следственные связи. В этом смысле аналитик создает новое знание о том фрагменте реальности, который находится в поле его профессионального интереса, выступая де факто исследователем своей предметной области.

Вместе с тем существуют и принципиальные различия между аналитикой и наукой. Научный анализ призван выявлять, прежде всего, фундаментальные, объективные закономерности изучаемой области, повторяющиеся, существенные связи объектов, обобщенные параметры процессов и т.п.

Информационная аналитика, опираясь на научное знание, общие закономерности, чаще всего имеет дело с феноменологией бытия, осуществляя оценку фактов и событий, прогнозируя их развитие с учетом не только обобщенных типичных параметров, но и целого спектра факторов, включая субъективно-личностные, случайные влияния, а также сознательные акции конкурирующих сил, противоборство

интересов, активное вмешательство социальных технологий и т.п. Существенную роль играет и фактор времени. Производство научного знания осуществляется в том специфическом режиме времени, который продиктован непредсказуемостью эвристических процессов познающего человеческого интеллекта, логикой и темпами научного дискурса. Информационная аналитика работает в режиме реального времени – времени жизнедеятельности своей предметной области (политики, экономики, бизнеса) и в соответствие с темпом необходимых управленческих реакций на динамику событий, происходящих в данной области.

С одной стороны, академические и отраслевые научно-исследовательские институты, разрабатывавшие фундаментальные и прикладные проблемы в тех областях знания, которые востребованы современной жизнью, практикой управления, так и не стали базовой структурой в системе формирующихся аналитических служб. И это не смотря на то, что еще в дореформенные времена Академия наук и ведущие НИИ рассматривались как инстанции для проведения экспертиз, им предъявлялись партийно-правительственные заказы на разработку научных обоснований для тех или иных проектов, концепций и планов, оценки и критики зарубежного опыта и т.д. С другой стороны, именно ученые, сотрудники академических институтов, НИИ, вузов в значительной степени пополнили ряды аналитиков при госструктурах, СМИ, в коммерческих фирмах, политических партиях и т.п.

Анализ этих факторов – самостоятельная научная проблема, однако нельзя не упомянуть наиболее значимые тенденции. Тенденция социализации информационной аналитики, объективно закономерный процесс, характеризующий новую отрасль в стадии ее становления. Составляющими процесса социализации информационной аналитики являются социальные, социокультурные, социально психологические реакции общества на данную отрасль. Появление новой сферы профессиональной деятельности (информационная аналитика) ставит перед обществом аксиологические, психологические, культурологические, социометрические проблемы:

- возникает необходимость социальной оценки значимости информационной аналитики, что требует ее позиционирования в ряду других, близких отраслей, выработки шкалы социальной оценки, построения системы социальных приоритетов и т.п. с учетом ценности тех целей, которые данная деятельность позволяет достичь;

- формируются эмоциональные реакции, ожидания, общепринятые нормы поведения в связи с данной отраслью;

- ценностные и социально-психологические реакции транслируются в область культурных норм и традиций, национальных форм социального бытия, включаются в систему мифов и ритуалов и т.п.;

- выстроенные приоритеты, оценки, престижность новой отрасли позволяют определять ее социометрические параметры (интенсивность роста социальных институтов, связанных с новой отраслью, темпы и масштабы рекрутинга специалистов-профессионалов, пользователей ее продукции).

Все эти проблемы характерны и для этапа становления отечественной информационной аналитики. Несомненно, итогом 90-х явилось достаточно широкое общественное признание социального статуса информационной аналитики, характеризующееся целым рядом признаков (информированность общества о

существовании аналитики, признание феномена аналитики как инструмента управления сложными процессами, средства раскрытия сути происходящих событий и прогнозирования их дальнейшего развития, формирование представления о профессиональном аналитике как эксперте, владеющим эксклюзивным знанием, к мнению которого необходимо прислушиваться как сильным мира сего, так и рядовым гражданам и т.п.).

За эти годы в России сформировался и социальный слой реальных и потенциальных клиентов, профессиональных потребителей информационно-аналитических продуктов и услуг, постепенно формируется представление об информационной аналитике как необходимом компоненте культуры управления, предпринимательской деятельности, инструменте современного менеджмента, составной части корпоративной культуры и т.п. Российское общество даже за столь краткий исторический период (90-е гг.) обрело достаточно разнообразный опыт в контактах с информационной аналитикой, чтобы осознать тот факт, что информационная аналитика может быть мощным и даже социально опасным орудием. Отметим, что широкая общественность имела возможность наблюдать применение аналитики, аналитического сопровождения в политической, экономической конкурентной борьбе, в процедурах лоббирования чьих-то интересов при принятии решений в самых высоких сферах отечественной политики, в массовых рекламных кампаниях, в кампаниях по манипуляции бщественным мнением, когда сталкивались мнения различно ангажированных аналитиков, в крупномасштабных и локальных информационных войнах, целенаправленных «сливах» компромата, многоходовых дезинформационных акциях и т.п., сценарии которых тщательно готовились аналитиками противоборствующих лагерей.

В полном соответствии социального и научно-технического прогресса информатизация вывела на историческую арену виртуальные, социально-информационные технологии, способные повысить уровень социальной управляемости, обеспечить новый информационный режим. Сущность понятия «новый информационный режим» заключается прежде всего в качественно ином уровне интеллектуализации информационного пространства (ноосферы), необходимом для устойчивого развития общества, повышения меры его управляемости, нейтрализации фактора индетерминизма социальных процессов. Цель интеллектуализации заключается в создании системы производства и передачи на входы управляющих блоков социума смыслосодержащей информации, максимально отвечающей задачи формирования и принятия управленческих решений. Интеллектуализация информационного пространства осуществима при следующих условиях:

- оптимальном структурировании мирового информационного пространства за счет упорядочения глобальной информационной инфраструктуры;

- интеграции и структурировании мировых информационных ресурсов;

- собственно интеллектуализации информационных потоков и процедур переработки информации.

Некоторые из этих условий еще только намечены, но уже сегодня, очевидно, что их базовый элемент – совокупность информационных технологий во главе с информационной аналитикой. Во всех значимых точках пересечения и концентрации информационных потоков должны быть созданы узлы интеллектуальной переработки

информации, формирующие интеллектуализированную инфраструктуру информационного пространства.

Экстраполируя параметры и темпы прогресса в области компьютерных и телекоммуникационных техники и технологий и возрастающую виртуализацию всех сфер человеческой деятельности, можно определить информационную аналитику и информационный мониторинг как перспективные технологии социального управления XXI века.

ЧАСТЬ 2
АНАЛИТИЧЕСКАЯ РАБОТА В СФЕРЕ БЕЗОПАСНОСТИ

Глава 2. Содержание аналитической работы

2.1. Анализ и основные понятия

Зачастую человек затрудняется сходу объяснить, что он понимает под тем или иным словом. Более того, его понимание может несколько изменяться со временем и от ситуации к ситуации. Поэтому люди, как правило, недопонимают друг друга, даже если действительно хотят разобраться в том, что им говорят. Во многих случаях это не важно. Но в условиях, когда нюансы смысла приобретают большое значение, должны приниматься меры к тому, чтобы понятия, стоящие за используемыми словами, более определённо и устойчиво соотносились между собой, то есть образовывали не совокупность, а **систему**.

Ниже предпринимается попытка привести в систему основные понятия, используемые в формальном и неформальном анализе. В химии анализ есть выяснение состава соединения или смеси. В умозрительной деятельности анализ есть расширение представлений о некоторых сущностях путем обработки уже имеющихся сведений о них, а также обработки обобщенных сведений о типе, к которому они относятся. Более конкретно под анализом некоторого феномена можно понимать выяснение значений его характеристик, не обнаруживаемых напрямую.

Аналитические технологии разделяются на формальные и неформальные. Формальные технологии компьютеризуются, неформальные реализуются при решающем участии человеческого интеллекта (который может получать при этом компьютерную поддержку). Формальный анализ осуществляется индивидуумом на уровне сознания, неформальный – в основном на уровне подсознания. Формальные операции (не только аналитические) состоят в некоторых перестановках и замещениях, проводимых по четким правилам и легко доступных для компьютеризации.

Анализ (формальный, неформальный) направлен либо на выяснение прошлого, либо на разгадывание будущего, либо на получение более полной картины существующего в текущий момент времени. Как правило, разработчики формальных методов анализа склонны слишком высоко оценивать их возможности и видеть больше областей их эффективного применения, чем есть в действительности. Анализ всегда выполняется в соответствии с некоторым подходом к структурированию мира. Этот подход иначе называется парадигмой.

Парадигма – от греческого paradeigma («пример», «образец»). Понятие парадигмы было введено в аналитической грамматике и обозначало образцы словоизменения

(склонения, спряжения). Новое значение слову «парадигма» предложил Т. Кун в книге "Структура научных революций" (русс. перевод 1975, стр. 11): «Под парадигмами я подразумеваю признанные всеми научные достижения, которые в течение определенного времени дают модель постановки проблем и их решений научному сообществу». С. Бир («Мозг фирмы», М., 1993: стр. 219): «Парадигма – это образец; в нашем случае – образец фундаментального подхода к решению определенной общей проблемы, который может быть полезен для множества различных ситуаций». В числе популярных парагдигм структурирования мира следует назвать прежде всего «системный подход» – рассмотрение различных сущностей как систем, то есть устойчивых образований, которые характеризуются следующими качествами:

1) отделены от остального мира четкими границами;

2) не пересекаются между собой;

3) взаимодействуют с остальным миром через свои «входы» и «выходы»;

4) состоят из не пересекающихся между собой подсистем, которые в совокупности образуют постоянную структуру.

С точки зрения системного подхода, любая сущность может рассматриваться как система. Любая система не есть сумма своих частей, а проявляет по сравнению с ними некоторые новые качества. Системный подход к исследованию некоторого феномена означает рассмотрение его «во всей полноте» и «во взаимосвязи» с другими феноменами.

Системный подход эффективен при рассмотрении технических объектов, но ведет к чрезмерным упрощениям, если его применяют к социальным феноменам. При рассмотрении различных социальных феноменов необходимо иметь в виду, что они:

1) обычно не имеют четких границ;

2) обычно пересекаются между собой;

3) обычно взаимодействуют с остальным миром не только через свои «входы» и «выходы»;

4) обычно состоят из пересекающихся между собой суб-феноменов, которые в совокупности не образуют постоянной структуры.

Системный анализ – формализованный вариант системного подхода. Системный анализ в узком смысле – построение нормализованного или формального описания некоторой сущности, рассматриваемой в качестве системы.

Системный анализ в широком смысле – получение новых сведений о некоторых сущностях путем формальных операций над формальными описаниями этих сущностей, полученными путем интерпретации этих сущностей как систем.

В аналитической работе системный анализ годится, к примеру, для разгадывания конструкции некоторого сложного технического устройства. Если же его пытаются использовать, к примеру, в исследовании работы некоторого учреждения, то получаются жалкие (хотя и наукообразные) результаты – поскольку в учреждении:

- различается структура формальная и структура неформальная;

- формальная структура сама по себе не вполне работоспособна;

- неформальная структура расплывчата и неустойчива.

Далее рассматриваются основные понятия, используемые в аналитической работе.

Феномен (явление) – любая сущность, которая имеет достаточную протяженность в пространстве и времени и достаточное своеобразие на фоне прочих сущностей, чтобы быть замеченной. То есть выделение или невыделение феномена определяется характеристиками наблюдающего его субъекта.

Объект – феномен, который не изменяется или в котором можно выделить неизменные компоненты. Часть объекта – входящая в объект сущность, представляющая собой нечто физически связанное. Часть объекта – не то же, что и часть системы: часть системы характеризуется некоторой функцией по отношению к целому, а часть объекта – не обязательно. Части объекта, части системы не перекрываются между собой в пространстве. В феномене могут выделяться компоненты – составляющие его сущности любой природы. Отличия компонента от части:

1) компонент феномена не обязательно представляет нечто физически целое:

2) компоненты феномена могут взаимно перекрываться в пространстве:

Атрибуты феномена (объекта, субъекта, системы, процесса) – типовые компоненты его описания: название, тип, структура и прочее.

Свойства (параметры) феномена (объекта, субъекта, системы, процесса) – компоненты его описания, характеризующиеся названием и значением.

Состояние феномена – набор значений его свойств, имеющих место одновременно.

Процесс – изменение некоторых сущностей (последовательная смена их состояний и пр.), осуществляющееся непрерывно или пошагово. Можно строить картину мира, в которой то, что обычно считают объектом, рассматривается как частный случай процесса.

Событие – (скачкообразное) изменение некоторых сущностей (смена одного состояния на другое), реализующееся в один шаг. Можно считать событие элементарным процессом. Либо можно условиться, что изменение реализующееся не в один шаг, а в несколько, есть процесс, а не событие. Либо можно принять, что событие может реализовываться в несколько шагов и что нет четкой границы между событием и

процессом. Событие имеет начало и конец либо является мгновенным, а процесс не обязательно имеет начало и/или конец. Процесс может делиться на события.

Субъект – сущность, способная как целое отражать свое окружение и/или себя самого и намеренно изменять это окружение и/или себя самого и/или свое место в этом окружении. (Если субъект не способен изменять себя, то ему незачем себя отражать; если он не способен изменять свое окружение и/или свое место в нем, то ему незачем отражать это окружение; а если субъекту незачем отражать, то и способность к отражению не может развиться до высокой степени сложности. Сущность, которая способна отражать, но не изменять, – это отражающий объект, а не субъект.) Субъект может включать в себя другие субъекты, входить в другие субъекты в качестве части. Субъект, состоящий из других субъектов, возникает при установлении между ними определенных отношений. Субъект, состоящий из других субъектов, может превратиться в объект (потерять субъектность), если определенные отношения между составляющими его субъектами перестанут существовать.

Атрибуты субъекта: цели, ценности, представления о себе, представления о внешнем мире. Нет четкой границы между субъектностью и объектностью. Одна и та же сущность может в отношении одних феноменов выступать как субъект, в отношении других – как объект. К примеру, если на человека неожиданно падает с дерева ябляко, то оно сталкивается с ним как с объектом, а если человек срывает с дерева яблоко, он действует как субъект.

Субстрат феномена – материя, являющаяся носителем этого феномена. На одном и том же субстрате в разное время могут иметь место разные феномены. Феномены выделяются в некотором пространстве – физическом или виртуальном. Пространство – то, в чем можно что-то размещать. Виртуальное пространство – совокупность мест, задаваемых некоторой совокупность взаимосвязанных феноменов. Всякое место может быть занятым феноменом или оставаться свободным.

Фактор – то, что влияет на феномен и/или на субъект, принимающий решение. Влияние – вызывание изменений. Влияние фактора A на сущность B может быть:

- определяющее: задающее состояния B;

- решающее: незначительно искажаемое другими факторами;

- преобладающее: превосходящее все прочие влияния вместе взятые;

- наибольшее: превосходящее любое из прочих влияний;

- существенное: входящее в группу факторов, совокупно оказывающих решающее влияние;

- заметное: легко различимое по последствиям;

- малозаметное: трудно различимое по последствиям;

- незаметное: теоретически имеющееся, но фактически неразличимое.

Система – сущность, которая мыслится как обладающая следующими особенностями:

1) отделена от остального мира некоторой границей;

2) воспринимает воздействие внешнего мира через особые каналы, называемые «входами»;

3) воздействует на остальной мир через особые каналы, называемые «выходами»;

4) характеризуется относительной устойчивостью своей структуры.

Структура системы – совокупность ее частей и их взаимных связей. Организация системы – неизменный компонент ее структуры, отличающий ее от других систем. В системах различаются процессы трех уровней:

- затрагивающие значения свойств, но не структуру системы;

- затрагивающие структуру системы, но не ее организацию;

- затрагивающие организацию системы (то есть превращающие ее в другую систему).

Структура процесса – совокупность состояний и их взаимных связей. Целая сущность – такая, которая имеет полный набор компонентов, составляющих объем понятия о нормальном состоянии этой сущности. Понятие целого применимо к одним сущностям и неприменимо к другим. Его можно применять лишь к неоднородным сущностям. Сущность остается таковой (хотя и не-целой) при утрате одних своих компонентов и перестает быть таковой при утрате других своих компонентов. К примеру, веревка не станет нецелой (не в смысле «поврежденной», а в смысле «неполносоставной»), если от нее отрезать кусок. Цепь не станет нецелой, если отделить нее несколько крайних звеньев. Человек не станет нецелым, если, к примеру, срезать у него прядь волос, но станет, если, к примеру, лишить его руки. Если не лишать человека руки, но заставить его голодать так, что он потеряет значительную долю своего веса, он все еще будет представлять собой целое. Объекты бывают:

1) однородные;

неоднородные:

- с границами между частями: из одинаковых частей, из неодинаковых частей;

- с плавным изменением свойств при переходе от одной точки объекта к другой;

2) неделимые (попытка отделения части уничтожает эту часть):

- делимые в любом месте;

- делимые по границам между частями.

Части объекта бывают: слитные, соединенные, соприкасающиеся, разделенные.

О различиях между причиной и условием. Причина – то, что даёт толчок событиям. Условие – отсутствие препятствия или ресурс, расходуемый при толчке или в процессе разворачивания события. Причины, условия разделяются на необходимые и достаточные. Распространено деление причин социальных феноменов на субъективные и объективные. Субъективные – те, которые зависят от действий людей (соответственно от воззрений, способностей и других человеческих качеств), объективные – те, которые от этого не зависят. Такое деление является очень приблизительным, удобным для оправданий, но подавляющим инициативу и творческое воображение. Дело в том, что сама граница между зависимым и

независимым от людей определяется воззрениями, способностями и др. человеческими качествами. Продуктивнее считать, что от человека зависит почти всё, но что-то зависит больше, а что-то меньше; что в отношении некоторых вещей есть готовые средства влияния, а в отношении некоторых других они лишь в принципе возможны. В причинах события надо различать следующее:

1. Наличие и силу факторов, которые способствовали тому, чтобы событие произошло.

2. Отсутствие или слабость факторов, которые препятствовали тому, чтобы событие произошло.

О целом обычно приходится судить по некоторым сведениям о его частях. При этом легко впасть в большую ошибку, поскольку некоторые части могут не только значительно отличаться своим характером от целого, но даже быть чуждыми ему. К примеру, если в некоторой социальной группе имеет хождение определенный идеологический документ, это еще не значит, что вся эта группа или, по крайней мере, большая ее часть руководствуется им, хотя ради каких-то манипулятивных целей можно представлять положение дел именно так.

Аналитическая работа. Аналитическая работа – составная часть творческой деятельности. Она предназначена для оценки информации и подготовки принятия решений. Составляет основное содержание повседневной работы каждого руководителя и работника. Аналитическая работа, как процесс познания объективной реальности, осуществляется по законам диалектики, формальной логики, с применением общенаучных методов исследования.

Содержание аналитической работы – приведение разрозненных сведений в логически обоснованную систему зависимостей (пространственно-временных, причинно-следственных и иных), позволяющих дать правильную оценку, как всей совокупности фактов, так и каждому из них в отдельности.

Средства аналитической работы – это законы и методы мыслительной деятельности, а также иные технические средства, на основе и с помощью которых осуществляется обработка фактических данных с более высоким качеством, позволяющим извлечь из нее все, что она может дать.

Формы аналитической работы – организационные особенности осуществления аналитической работы, обусловленные целями, средствами и результатами ее проведения, образующие систему аналитического слежения за состоянием и развитием обстановки.

Процесс аналитической работы – совокупность мыслительных операций, осуществляемых в определенной последовательности с использованием аналитических средств, приводящих к достижению целей и задач исследования.

Технология аналитической работы – получение нового знания (выводной информации), обеспечивающего сложный процесс исследования, имеющий определенную логическую последовательность.

Под проведением исследования понимается система взаимосвязанных рабочих операций, которые образуют технологический цикл отбора, группировки фактов о событиях, явлениях, процессах, где каждый факт обретает свое место и связан с

предшествующими и последующими обстоятельствами в пространственно-временной и причинно-следственной зависимости. Обобщение фактов, их научная обоснованная систематизация позволяют дать правильную оценку, как всей совокупности фактов, так и каждому из них в отдельности.

Анализ собранных материалов в соответствии с целями и задачами исследования – это основной этап аналитической работы, на котором осуществляется осмысление материала, выработка новой выводной информации, формирование предложений по практическому их применению и документированию результатов исследования.

Анализ информации – совокупность методов формирования фактических данных, обеспечивающих их сравнимость (сопоставляемость), объективную оценку и выработку новой выводной информации.

Выработка новой информации – это извлечение содержания из всей массы исходных данных, отыскание причинно-следственных и пространственно-временных связей и взаимосвязей между сопоставляемыми сведениями.

Документирование результатов исследования – фиксация в установленном порядке результатов исследования с помощью системы обозначений, придающей описанию строгую форму, наглядность, логичность, краткость, ясность и отвечающей целям и задачам исследования.

Апробирование результатов исследования – проверочная процедура, направленная для выяснения качественных характеристик результатов исследования, возможностей реализации и внедрения их в практику.

Реализация результатов исследования – это передача результатов исследования в удобной для внедрения форме в практику работы заинтересованных лиц, обеспечивающих повышение эффективности их деятельности.

Проверка, утверждение и внедрение результатов аналитической работы – это завершающий этап процесса исследования, на котором выявляются недостатки в аналитической работе, осуществляется их устранение и дается оценка качеству полученных результатов.

2.2. Принципы аналитической работы

Если два политика публично враждуют между собой, это не значит, что они на самом деле враги. Возможно, они сговорились изображать враждебность, чтобы вводить в заблуждение своих действительных противников и массу зрителей.

Если некий популярный ведущий телепередачи энергично критикует чиновников, богачей, «демократов», это вовсе не свидетельствует о том, что он оппозиционер и что те не могут заставить его замолчать. Это, скорее всего, значит лишь то, что ему поручили приобрести доверие в народе, чтобы он сумел на ближайших выборах в ключевой момент убедительно призвать народ голосовать за кого-то из той самой категории деятелей, которую он интенсивно грызет.

Если президент отправляет в отставку правительство, из этого не обязательно следует, что он решил поменять курс или не доволен деятельностью министров. Это может значить, что он решил изобразить политическую активность (привлечь внимание к своей персоне, напомнить всем, «кто в доме хозяин»), зародить у многих надежду на перемену к лучшему, а заодно услужить соратникам, которым надоело отбиваться за всех на переднем крае и каждодневно ханжествовать перед телекамерами и захотелось спокойно в тени пожать плоды своих приобретательских усилий.

Если некоторые члены команды президента уходят из его администрации на должности, на которых больше шансов удержаться после смены власти, это не является верным признаком того, что дело идет к скорому освобождению места действующим главой государства: обстоятельства ухода членов команды могут быть совсем не такими, какими их изображают в средствах массовой информации и в частных разговорах. Перевод из ближнего окружения на периферию может быть средством, которым глава государства распространяет свое влияние. У лидера есть интерес в том, чтобы дать поработать вблизи себя большому количеству людей: присмотреться к ним, сделать их лично ему обязанными, повязать их общими сомнительными делами.

Иными словами, видимая часть вещей не всегда соответствует их сути, и надо предпринимать особые усилия, чтобы не впадать в заблуждение. Аналитик должен руководствоваться следующими принципами:

1. Не принимать ничего на веру. Опасаться неосознанного перенятия массовых заблуждений. Подвергать критическому разбору устоявшиеся мнения.

2. Распознавать попытки скрытого влияния на себя со стороны различных субъектов.

3. Не надеяться на помощь ученых. Учитывать слабости "нормальной науки", ограниченность возможностей всякой теории.

4. Вырабатывать у себя некоторое более или менее четко выраженное понимание сути человека и общества (чем менее определённым и развитым является это понимание, тем в большей степени всякое собственное мнение о текущих событиях является следствием преобладающих влияний).

5. Обращать внимание на аномалии, исключения из правил. Искать необычное в обычном.

6. Обращать внимание на детали. То, что представляется мелкой ошибкой, недоработкой, случайностью, на самом деле может быть проявлением скрытой сути.

7. При исследовании важных предметов искать несовпадающие мнения о них. Учитывать, что более правильное мнение не всегда является более аргументированным, лучше оформленным и шире распространенным.

8. Не перегружать себя работой. Проблем всегда больше, чем аналитик в состоянии решить; доступных сведений всегда больше, чем аналитик в состоянии обработать. Лучшие мысли приходят по преимуществу в свежую, не слишком занятую голову.

Уровни аналитической работы. Выделяются следующие уровни сложности познавательного мышления:

- работа в рамках существующих теорий;

- доработка существующих теорий;

- создание новых теорий в рамках существующих парадигм;

- создание новых парадигм.

Соответственно выделяются следующие уровни аналитической работы:

- аналитика нормального уровня: с использованием и доработкой существующих обобщенных представлений;

- аналитика высокого уровня: с обновлением обобщенных представлений в рамках существующей парадигмы;

- аналитика особо высокого уровня: с использованием разных существующих парадигм и созданием новых.

На 1-м уровне способны проявить себя многие умные люди, прошедшие специальную подготовку. 2-й уровень предполагает склонность к теоретизированию и готовность браться за масштабные задачи. 3-й уровень – удел индивидуумов, отмеченных чертами гениальности (понимаемой как специфический «раскрепощенный» склад ума и не обязательно выливающейся в выдающиеся творческие достижения). Их нужно всего 3–5 человек на всю аналитическую службу безопасности, но не всегда набирается и столько. Между тем, эту службу можно лишь в том случае считать полноценной, если такие люди попали в нее, заняли не последние должности и не имеют необходимости скрывать свои особенные качества.

Аналитическую работу на парадигмальном уровне вредно отделять от работы научно-философской. Первая обеспечивает вторую проблемами, фактами и стимулами, вторая первую – практическими идеями. Аналитику, работающему на парадигмальном уровне, по большому счету безразлично, что анализировать: лишь бы был творческий интерес, хорошо платили и давали время разобраться в предметной области.

Искусство сомнения. Склонность сомневаться в достоверности различных представлений называется скептицизмом. Скептицизм следует отличать от мнительности (которая тоже, впрочем, уместна) – склонности сомневаться в искренности, добросовестности и надежности людей. А также от критицизма (склонности во всем выискивать недостатки) и пренебрежительного отношения к мнениям и достижениям других (это никогда не бывает уместно). Могут быть выделены следующие уровни сомнения:

1. Сомнение в частностях: величинах, пропорциях, расстановке акцентов.

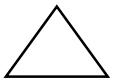
2. Сомнение в направлении: попытка выявить противоположное – «да» вместо «нет», «нет» вместо «да».

3. Сомнение в охвате: то, что представляется исчерпывающим, может оказаться частным случаем чего-то еще более общего.

Примеры из науки:

- геометрия Евклида → геометрия Лобачевского
- механика Ньютона → механика Эйнштейна

4. Сомнение в корректности структуризации предметной области, в адекватности системы понятий:

вместо возможно или 

Отличие интеллектуально талантливого человека – в способности переживать сомнения 3-го и 4-го уровней. В скептицизме надо различать:

- признание сомнительным чего-то конкретного;

- принципиальную готовность усомниться в чем угодно;

- предполагание возможной достоверности чего-то, признанного ложным;

- поиск и исследование альтернативных объяснений.

Не требуется больших усилий, чтобы признавать сомнительным всякий факт и всякое утверждение, но человек не в состоянии исследовать достоверность всякого факта и всякого обобщения, с которыми ему приходится работать. Таким образом, существует проблема оптимального распределения ограниченного интеллектуального ресурса между проверкой фактов и обобщений и их использованием. Сомнение усложняет деятельность и при неуместном употреблении отрицательно отражается на ее качестве.

Обращение внимания на мелочи. Расследование почти всякой большой катастрофы (стихийной, технической или социальной) приводит к выводу, что задолго до того, как она разразилась, имели место признаки, позволявшие сделать довольно убедительное заключение о ее возможности или даже о ее неизбежности. Более того, иногда находились люди, которые такое заключение делали и тщетно добивались внимания тех, у кого была достаточная власть для принятия защитных мер. Правда, это вовсе не означает, что люди, обладавшие властью, делали ошибки: возможно, они обращали внимание на какие-то другие обстоятельства или следовали более правдоподобным рекомендациям каких-то других предостерегающих и тем самым спасали общество от какой-то другой катастрофы. Во всякий момент времени в обществе существуют зачатки очень разных тенденций (в том числе взаимно противоположно направленных), большая часть из которых никогда не разовьется сколько-нибудь значительно, причем не из-за того, что кто-то намеренно ее остановит, а из-за неблагоприятного стечения обстоятельств.

Из этого следует, что лучше принимать защитные меры с широким спектром действия, но из этого не следует, что малополезно пробовать распознать что-то скрытое, зарождающееся или вовсе еще не существующее, но уже имеющее предпосылки для своего возникновения.

Работа с фактами. Фактами можно доказать и опровергнуть все, что угодно. Особенно если использовать не все факты, относящиеся к рассматриваемому предмету. При исследовании сложных явлений нередко на всякий важный факт отыскивается другой факт – с противоположным смыслом. Также случаются ситуации, когда один и тот же факт применяется для обоснования противоположных позиций. Преимущество получает тот из оппонентов, кто первый привлечет факт на свою сторону. Восприятие факта индивидуумом зависит от уже имеющихся у этого индивидуума воззрений. В одном и том же явлении разные люди увидят разные факты. Вдобавок со временем выясняется, что некоторые факты – ложные (одни – вследствие ошибок, другие – вследствие лжи). В общем, перед фактами преклоняться не следует. Слово «факт» завораживает только людей с недоразвитым мышлением.

Качество анализа. Если собрать небольшую коллекцию текстов относящихся к некоторой проблеме, то можно быстро формировать правдоподобные аналитические записки по ней путем выдергивания и частичного перефразирования фрагментов из разных источников. Некоторые источники можно указывать (для демонстрации своего знакомства с ними и для того, чтобы подкреплять свои утверждения чужими мнениями), некоторые можно умалчивать (чтобы материал воспринимался как продукт собственных изысканий и размышлений). Если источники качественные, и обработка их проведена аккуратно, то результат обычно получается по крайней мере неплохой. При нехватке времени и отсутствии собственного оригинального и хорошо проработанного мнения это может быть приемлемо. Во вполне доступных текстах изложено огромное количество мнений по огромному множеству вопросов. Искусство правильно сделать выбор из чужих мнений – это немало. В отношении мнений различаются люди следующих типов:

1) способные воздерживаться от укрепления в каком-нибудь мнении, если для этого нет достаточных оснований;

2) способные менять мнение под влиянием корректных аргументов;

3) склонные непроизвольно и некритично приобретать и менять мнение;

4) склонные придерживаться однажды усвоенного мнения и проявлять безразличие к его критике.

Лучше не иметь никакого мнения, чем иметь некритично усвоенное. При заимствовании текстов важно не стать жертвой недобросовестности авторов. Возможные дефекты источников:

- ошибка рассуждений, расчетов, восприятия, вспоминания;

- намеренное дезинформирование, умалчивание;

- плагиат;

- имитация глубокомыслия;

- демагогия;

- розыгрыш.

Аналитическая служба и официальная идеология. Аналитику читать оппозиционную прессу обычно гораздо интереснее, чем официозную. Руководствование официальной идеологией в аналитике отрицательно сказывается на качестве работы. Официальная идеология не может не быть упрощенной: во-первых, потому что она массовая, то есть рассчитанная на усвоение ее средним человеком; во-вторых, потому что она представляет собой соединение кусков разного происхождения, компромиссный продукт творческих усилий множества разработчиков. Аналитиками особо высокого уровня могут быть только вольнодумцы. Пренебрежение официальной идеологией не означает пренебрежительного отношения к государству. Эта идеология – лишь инструмент государства, заменяемый по мере надобности, а не какая-то священная «основа». Аналитическая служба – не инструмент, а орган государства. Она «первичнее» официальной идеологии и даже может участвовать в ее разработке.

2.3. Применение логических законов и правил в аналитической работе

Текст аналитической работы отличается от всякого другого, прежде всего, своей логичностью. Поэтому какие бы ошибки с точки зрения логики ни делали авторы диссертационных работ при описании хода исследования, всегда можно доказать, что любая ошибка такого рода сводится в конечном счете к нарушению требований того или иного логического закона: закона тождества, закона противоречия, закона исключенного третьего и закона достаточного основания. Поэтому имеет смысл рассмотреть эти законы более подробно.

Поскольку в научном тексте используются понятия и суждения, очевидно, что именно эти смысловые единицы должны удовлетворять требованию определенности. Это требование находит свое выражение в **законе тождества**, согласно которому предмет мысли в пределах одного рассуждения должен оставаться неизменным, т. е. А есть А (А=А), где А – мысль. Такой закон требует, чтобы в ходе сообщения все понятия и суждения носили однозначный характер, исключающий двусмысленность и неопределенность.

На первый взгляд содержащееся в законе тождества требование представляется предельно простым. В самом деле, надо лишь проявлять минимальную строгость, не смешивая различные (пусть даже и близкие) мысли, отграничивая их друг от друга с достаточной степенью четкости. Однако по ряду причин эта простота является обманчивой.

К таким причинам, прежде всего, относится большой слой явлений языка и речи. Ведь в любом тексте мы имеем дело не с «чистой» мыслью, а с единством ее содержания и словесной формы. Между тем хорошо известно, что внешне одинаковые словесные конструкции могут иметь разное содержание и, наоборот, одна и та же мысль может быть выражена по-разному. Первое явление называется омонимией, второе – синонимией. Омонимия делает возможным неправомерное отождествление объективно различного, а синонимия – ошибочное различение тождественного.

Отождествление различных понятий представляет собой одну из наиболее распространенных логических ошибок в научном тесте – подмену понятия. Сущность этой ошибки состоит в том, что вместо данного понятия и под видом его употребляют

другое понятие. Причем эта подмена может быть как неосознанной, так и преднамеренной. Подмена понятия означает подмену предмета описания. Описание в этом случае будет относиться к разным предметам, хотя они будут ошибочно приниматься за один предмет.

В основе **закона противоречия** лежит качественная определенность вещей и явлений, относительная устойчивость их свойств. Отражая эту сторону действительности, закон противоречия требует, чтобы в процессе разговора мы не допускали противоречивых утверждений. Если, например, предмет А имеет определенное свойство, то в суждениях об этом предмете мы обязаны утверждать это свойство, а не отрицать его и не приписывать данному предмету того, чего у него нет. Закон противоречия для научной работы имеет огромное значение. Его сознательное использование помогает обнаруживать и устранять противоречия в объяснениях фактов и явлений, вырабатывать критическое отношение ко всякого рода неточностям и непоследовательности в сообщении научной информации.

Закон противоречия обычно используется в доказательствах: если установлено, что одно из противоположных суждений истинно, то отсюда вытекает, что другое суждение ложно. Уличение в противоречивости является сильнейшим аргументом против любых утверждений.

Однако закон противоречия не действует, если мы что-либо утверждаем и то же самое отрицаем относительно одного и того же предмета, но рассматриваемого 1) в разное время и 2) в разном отношении. Возьмем для иллюстрации первый случай, когда кто-либо утверждает, что «Дождь благоприятен для сельского хозяйства», а в другой раз этот же человек высказывает противоположную мысль: «Дождь неблагоприятен для сельского хозяйства». Но, то и другое высказывание может быть истинно. В первом случае имеется в виду весна (перед всходом растений). Во втором случае – осень (перед уборкой урожая).

В качестве примера второго случая возьмем ситуацию, когда о сотруднике Петрове можно сказать, что он хорошо знает английский язык, так как его знания удовлетворяют требованиям вуза. Однако этих знаний недостаточно для его работы в качестве переводчика. В этом случае можно утверждать: «Петров плохо знает английский язык». В этих суждениях знание Петровым английского языка рассматривается с точки зрения разных требований, т. е. один и тот же сотрудник, если его рассматривать в разных отношениях, дает основание для противоположных, но одинаково истинных оценок.

В научной работе нельзя игнорировать и требование **закона исключенного третьего**. Этот закон утверждает, что из двух противоречащих друг другу суждений одно из них ложно, а другое истинно. Третьего не дано. Он выражается формулой: «А есть либо В, либо не В». Например, если истинно суждение «Наша фирма является конкурентоспособной», то суждение «Наша фирма не является конкурентоспособной» – ложно. Такой закон не действует на противоположные суждения, т.е. на такие суждения, каждое из которых не просто отрицает другое, а сообщает сверх этого дополнительную информацию. Возьмем два суждения: «Этот лес хвойный» и «Этот лес смешанный». Здесь второе суждение не просто отрицает первое, а дает дополнительную информацию, т. е. речь идет не просто о том, что неверно, будто этот лес хвойный, но говорится, какой именно этот лес.

Важность закона исключенного третьего для ведения научной работы состоит в том, что он требует соблюдения последовательности в изложении фактов и не допускает противоречий. Такой закон формулирует важное требование к научному работнику: нельзя уклоняться от признания истинным одного из двух противоречащих друг другу суждений и искать нечто третье между ними. Если одно из них признано истинным, то другое необходимо признать ложным, а не искать третье, несуществующее суждение, так как третьего не дано. Важность соблюдения закона исключенного третьего для научных работников также и в том, что он требует от них ясных, определенных ответов, указывая на невозможность искать нечто среднее между утверждением чего-либо и отрицанием того же самого.

Требование доказательности научных выводов, обоснованности суждений выражает **закон достаточного основания**, который формулируется следующим образом: всякая истинная мысль имеет достаточное основание. Достаточным основанием какой-либо мысли может служить любая другая мысль, из которой с необходимостью вытекает истинность данной мысли.

Почему говорят «достаточное основание», а не просто «основание»? Дело в том, что под одно и то же утверждение можно подвести бесконечно много оснований. Однако из них только некоторые могут рассматриваться как достаточные, если данное утверждение истинно. И ни одно не будет достаточным, если оно ложно. Таким образом, закон достаточного основания требует, чтобы всякое суждение, которое мы используем в научной работе, прежде чем быть принятым за истину, должно быть обосновано. Во всех случаях, когда мы утверждаем что-либо или убеждаем в чем-либо, мы всегда должны доказывать наши суждения, приводить достаточные основания, подтверждающие истинность наших высказываний, фиксируя внимание на высказываниях, обосновывающих истинность выдвигаемых положений, этот закон помогает отделить истинное от ложного и прийти к верному выводу.

Значительная часть научной информации носит характер выводных суждений, т. е. суждений, не полученных путем непосредственного восприятия каких-то фрагментов действительности, а выведенных из других суждений, которые как бы извлечены из их содержания. Логическим средством получения таких выводных знаний и является умозаключение, т. е. мыслительная операция, посредством которой из некоторого количества заданных суждений выводится иное суждение, определенным образом связанное с исходным. Все умозаключения можно квалифицировать как индуктивные и дедуктивные.

Поскольку большинство приводимых в научных текстах показателей являются итогом перечней отдельных примеров, есть необходимость привести способы обоснованности их использования в таких текстах, основываясь на рекомендациях, даваемых известным американским специалистом по ораторскому искусству Полем П. Сопером в книге «Основы искусства речи».

Первый способ – установить, правилен ли пример, положенный в основу обобщения, поскольку неправильность такого примера может резко подорвать доверие не только к данному обобщению, но и к самому автору научной работы.

Второй способ – выяснить, имеет ли пример отношение к заключению. Допустим, что краска марки А стоит дешевле, чем краска марок Б, В и Г. Казалось бы, неизбежен вывод, что краска марки А выгоднее других. Но такое заключение было бы

неправильным, потому что приведенные примеры не обладают качеством относимости к выводу. Они относимы только к заключению, что краска марки А самая дешевая. Лучшие качества краски других марок делает их более выгодными. Это одна из самых обычных ошибок в индуктивных заключениях.

Третий способ – определить, достаточно ли приведено примеров. Решение вопроса, достаточно ли взято примеров, зависит от их количества, способа отбора и видоизменяемости. Взяв наугад два случая некомпетентности отечественных бизнесменов, еще нельзя прийти к выводу, что все наши бизнесмены – люди некомпетентные. В России много тысяч предпринимателей. При отборе нескольких примеров большую роль играет фактор случайности. Российские бизнесмены, как и вообще все люди, очень различны.

Четвертый способ – установить, типичны ли подобранные примеры. Этот способ проверки имеет прямое отношение к изложенному выше. Достаточно или недостаточно примеров, зависит от того, насколько они типичны.

В научных исследованиях объектом исследования нередко выступают единичные, неповторимые по своим индивидуальным характеристикам события, предметы и явления. При их объяснении и оценке затруднено применение как *дедуктивных*, так и *индуктивных* рассуждений. В этом случае прибегают к умозаключению по **аналогии**, когда уподобляют новое единичное явление другому, известному и сходному с ним единичному явлению и распространяют на первое ранее полученную информацию.

В аналитических исследованиях аналогия приобретает значение важного для приумножения научных знаний типа умозаключения. История развития науки и техники показывает, что аналогия послужила основой для многих научных и технических открытий. Особую роль играет умозаключение по аналогии в общественно-исторических науках, приобретая нередко значение единственно возможного метода исследования.

Далеко не все аналогии логичны, поэтому необходима их проверка. Существуют два способа их проверки. Первый способ – действительно ли уместно сравнение явлений? Второй способ – нет ли существенного различия между ними? Два и более явлений могут быть существенно схожи и все же отличаться отсутствием подобия, необходимого с точки зрения доказываемого положения. Следующий очевидный абсурд, приводимый в качестве примера во многих учебниках логики, выявляет возможную в этом отношении ошибку: «Киты и слоны – млекопитающие, следовательно, и те и другие водятся на суше». Здесь наши обычные знания – защита от подобного ошибочного вывода.

Истина в том, что нет полной логической аналогии, ибо не бывает двух совершенно одинаковых совокупностей обстоятельств. Поэтому аналогией редко можно пользоваться, не обращаясь к другим видам доказательств.

Рассмотрим другой вариант индукции – *суждение о причинной зависимости*, которое играет особенно важную роль в научном тексте. Именно здесь чаще всего приходится фиксировать смену явлений.

Заключение о причине и есть логическое рассуждение о перемене: оно представляет вывод, что при данном положении вещей результатом будет то или иное заключение (от причины к следствию) или, что данное положение вещей вызвано известными

другими условиями (заключение от следствия к причине). Вариантом этих видов умозаключения будет вывод от следствия к следствию, если у того и другого одна общая причина.

В заключение от причины к следствию причина известна и из нее выводится следствие. В заключение от следствия к причине известно следствие и о причине делается вывод. В каждом спорном случае умозаключения о причинной зависимости применяются следующие правила проверки:

1. Возникает ли предполагаемое следствие, когда отсутствует предполагаемая причина? Если ответ – «да», то вы не вправе утверждать, что предшествующее явление – единственно возможная причина. Или нет никакой связи между двумя явлениями, или есть другая возможная причина.

2. Отсутствует ли предполагаемое следствие, когда предполагаемая причина налицо? Если ответ – «да», то вы не вправе утверждать, что последующее явление есть единственно возможное следствие. Или нет никакой связи между двумя явлениями, или есть другое возможное следствие.

3. Не представляет ли единственная связь между следствием и его предполагаемой причиной только случайное возникновение одного после другого? Этот способ позволяет выявить характерное заблуждение в умозаключении о причине, хорошо известное под названием «после этого, следовательно, по причине этого». Данная ошибка представляет форму беспечного обобщения отрывочных сведений.

4. Нет ли других возможных причин? Волнующая нас причина или ближайший повод явления обычно кажутся более очевидными, чем основная причина. Уклонение от установления основной причины – обычная форма уловок.

5. Нет ли других возможных последствий? В большинстве случаев заключение от причины к следствию представляет на самом деле предсказание будущих событий. В таких случаях абсолютная проверка невозможна.

Так как заключение от причины к следствию имеет в виду будущее, оно подвержено влиянию произвольного мышления, т. е. мышления, которое определяется желаниями и чаяниями. Уяснив основные варианты индукции, перейдем теперь к умозаключениям из общего положения, т. е. к дедукции. *Дедукция* – кратчайший путь к познанию. В этом ее характерное преимущество. Дедукция проста в том смысле, что состоит из трех суждений:

1) общего положения, именуемого большой посылкой;

2) связанного с ним суждения, ведущего к его применению под названием малой посылки;

3) заключения.

Весь этот трехзвенный процесс называется силлогизмом. Иногда одна из посылок или заключение не указываются. Этот сокращенный силлогизм называется *энтимемой*. Например: «Наше правительство не умеет работать, потому что все демократические правительства не умеют работать» (опущена малая посылка: наше правительство – демократическое). Чтобы восстановить энтимему в полный силлогизм, следует руководствоваться следующими правилами:

1) найти заключение и так его сформулировать, чтобы больший и меньший термины были четко выражены;

2) если опущена одна из посылок, установить, какая из них (большая или меньшая) имеется. Это делается путем проверки, какой из крайних терминов содержится в этом суждении;

3) зная, какая из посылок опущена, а также зная средний термин (он имеется в той посылке, которая дана), определить оба термина недостающей посылки.

Дедуктивные умозаключения проверяются двумя способами:

1) правильны ли посылки?

2) следует ли из них данный вывод?

Главное в научном исследовании – умение доказать свои суждения и опровергнуть (если потребуется) доводы оппонентов. Аргументирование, построенное на законах логики, помогает аналитику решить эти задачи.

Аргументирование – это сугубо логический процесс, суть которого в том, что в нем обосновывается истинность нашего суждения (того, что мы хотим доказать, т. е. тезиса доказательства) с помощью других суждений (т. е. аргументов, или, как их проще называют, доводов). Аргументация достигает цели, когда соблюдаются правила доказательства. Начнем с правил формулировки предмета нашего доказательства, т. е. с построения его тезиса.

Правило первое. Тезис доказательства нужно сформулировать ясно и четко. При этом нельзя допускать двусмысленность (например, формулировка следующего тезиса «Законы надо выполнять» – двусмысленна, ибо неясно, о каких законах идет речь: о законах природы или о законах общественной жизни, которые не зависят от воли людей, или о законах юридических, которые зависят только от воли граждан). Требование в формулировке тезиса не допускать двусмысленности – очень важно, ибо любая ошибка в выборе слова, возможность двоякого толкования фразы, нечеткая форма изложения мысли – все это может быть обращено против вас, когда вы хотите что-либо доказать.

Правило второе. В ходе доказательства тезис должен оставаться неизменным, т. е. должно доказываться одно и то же положение. Если это правило не выполнять, то вы свою мысль доказать не сможете. Значит, в течение всего доказательства нельзя отступать от первоначальной формулировки тезиса. Поэтому на протяжении всего доказательства вам вашу формулировку тезиса надо держать под контролем. Теперь укажем на основные ошибки в построении тезиса.

Ошибка первая – потеря тезиса. Сформулировав тезис, мы забываем его и переходим к иному тезису, прямо или косвенно связанному с первым, но в принципе уже другому положению. Затем затрагиваем третий факт, а от него переходим к четвертому и т. д. В конце концов, мы теряем исходную мысль, т. е. забываем, о чем начали спорить. Чтобы так не получилось, нужен постоянный самоконтроль, нужно не терять основную мысль и ход рассуждения. Сначала надо зафиксировать последовательную связь основных положений и в случае непроизвольного ухода в сторону вновь вернуться к исходному пункту доказательства.

Ошибка вторая – полная подмена тезиса. Выдвинув определенное положение, вы начинаете доказывать нечто другое, близкое или сходное по значению, т. е. вы подменяете основную мысль другой.

Ошибка третья – частичная подмена тезиса. Когда в ходе доказательства мы пытаемся видоизменить собственный тезис, сужая или смягчая свое первоначальное слишком общее, преувеличенное или излишне резкое утверждение.

Если в одних случаях под влиянием контраргументов мы стремимся смягчить свою очень резкую оценку, ибо в таком случае ее легче защищать, то в других случаях наблюдается обратная картина. Так, тезис оппонента нередко стараются видоизменить в сторону его усиления или расширения, поскольку в таком виде его легче опровергнуть. К аргументам, чтобы они были убедительными, предъявляются следующие требования:

– в качестве аргументов могут выступать лишь такие положения, истинность которых была доказана и ни у кого не вызывала сомнения, т. е. аргументы должны быть истинными;

– аргументы должны быть доказаны независимо от тезиса, т. е. должно соблюдаться правило их автономного обоснования;

– аргументы должны быть непротиворечивы;

– аргументы должны быть достаточны.

Итак, **требование истинности** аргументов определяется тем, что они выполняют роль фундамента, на котором строится все доказательство. Аргументы не должны вызывать сомнения в их бесспорности, или они должны быть доказаны ранее. Опытному критику достаточно поставить под сомнение хотя бы один из наших аргументов, как сразу ставится под угрозу весь ход нашего доказательства. Нарушение этого требования приводит к двум ошибкам. Первая из них носит название «ложный аргумент», т. е. использование в качестве аргумента несуществующего факта, ссылка на событие, которого не было, указание на несуществующих очевидцев и т. п. Вторая ошибка – «предвосхищение основания» – это когда истинность аргумента не устанавливается с несомненностью, а только предполагается. В этом случае в качестве аргументов используются недоказанные или произвольно взятые положения: ссылки на расхожее мнение или высказанные кем-то предположения, якобы доказывающие наше утверждение.

Требование автономности аргументов означает, что аргументы должны быть доказаны независимо от тезиса. Иначе сам аргумент надо будет доказывать. Поэтому, прежде чем доказывать тезис, следует проверить аргументы.

Требование непротиворечивости аргументов означает, что аргументы не должны противоречить друг другу.

Требование достаточности аргументов определяется тем, что аргументы в своей совокупности должны быть такими, чтобы из них с необходимостью вытекал доказываемый тезис. Нарушение этого требования часто заключается в том, что в ходе доказательства используют аргументы, логически не связанные с тезисом и потому не доказывающие его истинность. Это нарушение обозначают фразой: «не вытекает», «не

следует». Здесь бывает два вида ошибок.

Первая ошибка – недостаточность аргументов, когда отдельными фактами пытаются обосновать очень широкий тезис: обобщение в этом случае, всегда будет «слишком поспешным». Причина: недостаточный анализ фактического материала с целью отбора из множества фактов лишь достоверных и наиболее убедительно доказывающих наш тезис. Обычно оппоненту в этом случае говорят: «Чем еще вы это можете подтвердить?»

Вторая ошибка – чрезмерное доказательство. Принцип «чем больше аргументов, тем лучше» не всегда подходит. Трудно признать убедительными рассуждения, когда, стремясь во что бы то ни стало доказать свое предположение, увеличивают число аргументов.

Действуя, таким образом, вы незаметно для себя начнете брать явно противоречащие или слабо убедительные аргументы. Аргументация в данном случае всегда будет нелогичной или малоубедительной, поскольку «кто много доказывает, тот ничего не доказывает». Таким образом, достоверность аргументов надо понимать не в смысле их количества, а с учетом их весомости и убеждающей силы.

Очень часто допускаются ошибки в способах доказательства, т. е. ошибки в демонстрации. Это ошибки, связанные с отсутствием логической связи между аргументами и тезисом, т. е. отсутствием связи между тем, чем доказывают, по отношению к тому, что именно доказывают.

Часто случается, что человек приводит многочисленные факты, цитирует солидные документы, ссылается на авторитетные мнения. Создается внешнее впечатление, что его речь достаточно аргументирована. Однако при ближайшем рассмотрении оказывается, что концы с концами не сходятся. Исходные положения – аргументы – логически «не склеиваются» с конечным выводом – тезисом. В общем виде отсутствие логической связи между аргументами и тезисом называют ошибкой «*мнимого следования*».

Одна из форм такого несоответствия – *неоправданный логический переход от узкой области к более широкой области*. В аргументах, например, описывают свойства определенного сорта товара, а в тезисе необоснованно утверждают о свойствах данного товара в целом независимо от его сорта.

Другая форма несоответствия – *переход от сказанного с условием к сказанному безусловно*. Например, когда используются аргументы, справедливые лишь при определенных условиях, в определенное время или в определенном месте, а их считают верными при любых обстоятельствах.

В аналитическом исследовании очень часто приходится доказывать не истинность, а ложность суждения или неправильность доказательства других исследователей, т. е. *делать опровержение их доводов*. Опровержение, таким образом, направлено на разрушение доказательства других исследователей путем установления ложности или необоснованности их утверждений.

Поскольку операция опровержения направлена на разрушение ранее состоявшегося доказательства, то в зависимости от целей критического разбирательства оно может быть выполнено следующими тремя способами: критикой тезиса, критикой аргументов

и критикой демонстрации.

Первый способ – критика (опровержение) тезиса. Его цель – показать несостоятельность (ложность или ошибочность) выставленного пропонентом тезиса. Опровержение такого тезиса может быть прямым или косвенным. Прямое опровержение строится в форме рассуждения, получившего название «сведение к абсурду». Аргументация в этом случае протекает в следующем виде: вначале условно допускают истинность выдвинутого пропонентом положения и выводят логически вытекающее из него следствие. Рассуждают при этом примерно так: допустим, что пропонент прав и его тезис является истинным, но в этом случае из него вытекают такие-то и такие-то следствия. Если при сопоставлении следствий с фактами окажется, что они противоречат объективным данным, то тем самым их признают несостоятельными. На этой основе делают заключение о несостоятельности и самого тезиса, рассуждая по принципу: ложные следствия всегда свидетельствуют о ложности их основания.

В качестве примера опровергнем положение «Земля является плоскостью». Временно примем за истинное это утверждение. Из него следует, что Полярная звезда должна быть видна везде одинаково над горизонтом. Однако это противоречит установленному факту: на различной географической широте высота Полярной звезды над горизонтом различна. Значит, утверждение «Земля плоская» является несостоятельным, т. е. Земля не плоская.

В процессе аргументации прямое опровержение выполняет разрушительную функцию. С его помощью показывают несостоятельность тезиса пропонента, не выдвигая никакой идеи взамен.

Косвенное опровержение строится иным путем. Оппонент может прямо не анализировать тезис противоположной стороны, не проверяя ни аргументов, ни демонстрации пропонента. Он сосредоточивает внимание на тщательном и всестороннем обосновании собственного тезиса. Если аргументация основательна, то вслед за этим делается второй шаг – приходят к заключению о ложности тезиса пропонента. Такое опровержение применимо, разумеется, только в том случае, если тезис и антитезис регулируются принципом «третьего не дано», т. е. истинным может быть, лишь одно из двух доказываемых утверждений.

Рассмотрим теперь **второй способ** разрушения ранее состоявшегося доказательства, который называется «критика аргументов». Поскольку операция доказательства – это обоснование тезиса с помощью ранее установленных положений, следует пользоваться аргументами (доводами), истинность которых не вызывает сомнений. Если оппоненту удается показать ложность или сомнительность аргументов, то существенно ослабляется позиция пропонента, ибо такая критика показывает необоснованность его тезиса. Критика аргументов может выражаться в том, что оппонент указывает на неточное изложение фактов, двусмысленность процедуры обобщения статистических данных, выражает сомнения в авторитетности эксперта, на заключение которого ссылается пропонент и т. п.

Обоснованные сомнения в правильности доводов (аргументов) с необходимостью переносятся на тезис, который вытекает из таких доводов (аргументов), и потому он тоже расценивается как сомнительный и нуждается в новом самостоятельном подтверждении.

Критика демонстрации – это **третий способ** опровержения. В этом случае показывают, что в рассуждениях пропонента нет логической связи между аргументами и тезисом. Когда тезис не вытекает из аргументов, то он как бы повисает в воздухе и считается необоснованным. Как критика аргументов, так и критика демонстрации сами по себе лишь разрушают доказательство. Заявлять о том, что этим опровергается и сам тезис противоположной стороны, нельзя. О нем можно лишь сказать, что он требует нового обоснования, т. к. опирается на неубедительные доводы (аргументы) или доводы (аргументы) не имеют прямого отношения к тезису.

Таковы основные правила аргументирования, построенные с использованием основных правил логического доказательства и опровержения. Только соблюдая их, можно вести успешно полемику на страницах диссертационной работы.

Рассмотрим теперь **правила построения логических определений**, которые характерны для тезисов научных произведений. Чаще всего их дают через родовой признак и ближайшее видовое отличие. Обычно вначале называется родовое понятие, в которое определяемое понятие входит как составная часть. Затем называется тот признак определяемого понятия, который отличает его от всех ему подобных, причем этот признак должен быть самым важным и существенным. Чтобы дать правильное определение чему-либо, надо соблюдать несколько требований, которые принято называть правилами. *Правило соразмерности* требует, чтобы объем определяемого понятия был равен объему определяющего понятия. Иначе говоря, эти понятия должны находиться в отношении тождества. Например, если мы определим банкира как собственника капитала, в этом случае определяющее понятие будет значительно шире, чем определяемое, поскольку собственниками денежного капитала являются не только банкиры. Такую ошибку называют ошибкой слишком широкого определения.

Если при определении понятия мы прибегаем к другому понятию, которое в свою очередь определяется при помощи первого, то такое определение содержит в себе круг. Разновидностью круга в определении является *тавтология* – ошибочное определение, в котором определяющее понятие повторяет определяемое. Например, «Экономист – это лицо, занимающееся экономикой». Подобное определение не раскрывает содержания понятия. Если мы не знаем, что такое экономист, то указание на то, что этот человек занимается экономикой, ничего не прибавит к нашим знаниям.

В некоторых случаях при определении понятий указывается не один видовой признак, а несколько. Обычно это делается тогда, когда невозможно указать такой единственный признак, который отличал бы данное понятие от всех других и раскрывал бы существенным образом его содержание. Поэтому в таких случаях указывается несколько признаков, достаточных для отличия определяемого понятия и раскрытия его содержания.

Подлинно научное определение сложных явлений и фактов не может ограничиваться формально-логическими требованиями. Оно должно содержать оценку определяемых фактов, исключающую односторонний подход, присущий в недавнем прошлом всей отечественной науке. При этом следует также учитывать и особую специфику аналитических текстов.

2.4. Методы аналитической работы

В данной главе рассматриваются методы аналитической работы, применяемые аналитической службой (АС). Все эти методы используются или могут использоваться и для решения других задач, например в маркетинге, НИОКР, стратегическом планировании и прочее. Главная обязанность АС – предоставлять в распоряжение лица, принимающего решения (как правило, руководителя фирмы или менеджера высшего уровня управления – МВУУ) аналитическую информацию, способствующую принятию правильных, оптимальных решений. В действиях по выполнению этой обязанности можно выделить основные этапы, приведенные на рис. 1.

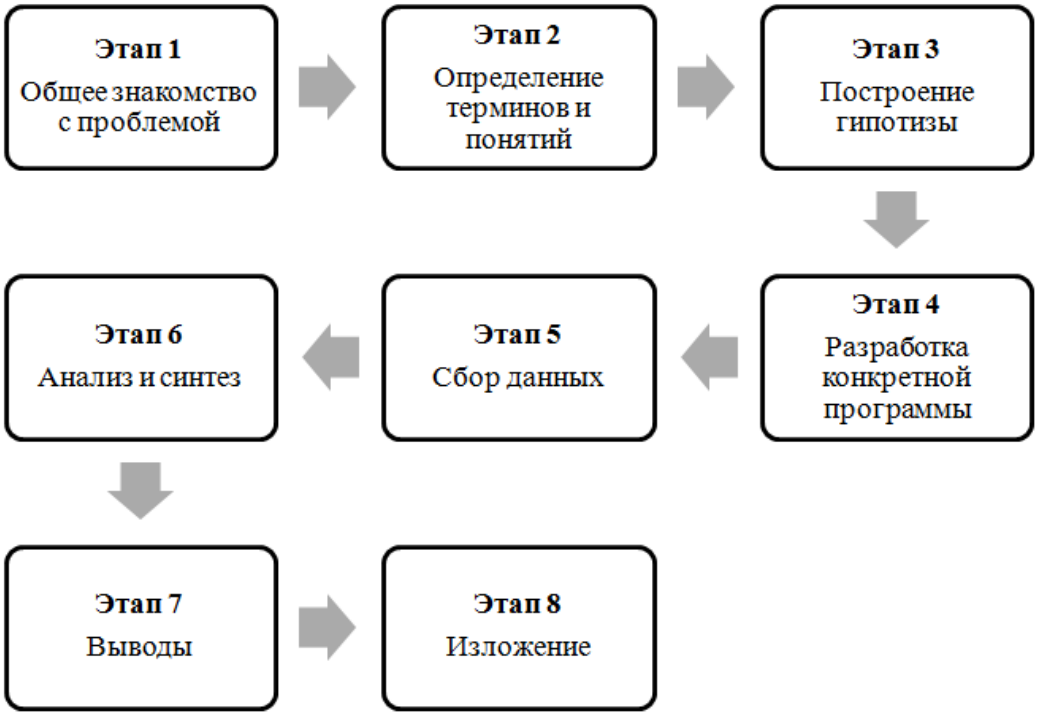


Рис. 1. Основные стадии аналитической работы

Этап 1. Общее знакомство с проблемой. Ознакомление с проблемой в целом, а также со смежными вопросами, изучение которых может оказаться полезным; составление общего плана работы с указанием срока выполнения, исполнителей и основных источников, которые предположительно могут быть использованы. Чтобы успешно справиться с заданием, очень важно вначале, при общем знакомстве с проблемой и составлении плана, действовать со знанием дела, обдуманно и рассудительно.

Этап 2. Определение терминов и понятий. Необходимо определить и объяснить тот или иной термин или понятие так, чтобы это было ясно нам самим, тем, кто контролирует нашу работу, и тем, кто пользуется нашей информацией.

Этап 3. Построение гипотезы. Рабочие гипотезы, выдвигаемые на этом этапе, обычно связаны с какими-либо конкретными вопросами, отвечая на которые можно проверить сами гипотезы. Многие считают построение гипотезы важнейшим моментом любого исследования как в области естественных или общественных наук, так и в области аналитической работы. Гипотезу можно рассматривать как положение. Обычно

отмечают три полезные стороны гипотезы:

– во-первых, тем самым облегчается уяснение проблемы. Установленное положение – прекрасное подспорье для памяти. Мы можем располагать значительными знаниями, помня определенное научное положение и не перегружая себя отдельными фактами;

– во-вторых, научное положение является основой для уяснения отдельных фактов или явлений, так как вскрывает существующую между ними связь. Мы можем осмыслить суть новых явлений, если выразим ее в знакомых нам понятиях;

– в-третьих, приемлемое научное положение всегда содержит некоторые моменты, выходящие за его рамки и образующие разумное и плодотворное основание для предвидения новых фактов и явлений. Короче говоря, приемлемое положение (или теория) помогает мобилизовать наши знания для использования в сфере не только чистой, но и «прикладной науки».

Все сказанное можно суммировать следующим образом: «Нет ничего более практичного, чем хорошая теория». Построение гипотезы, взятое в широком смысле, всегда присуще любой исследовательской работе. В самом начале исследования, когда вырабатывается общий план, мы исходим из определенных предположений (или гипотез) о том, какие факторы, возможно, играют важную роль и какие почти определенно не имеют отношения к делу. Аналогичными гипотезами мы руководствуемся при сборе и истолковании фактов, формулировании выводов и изложений.

Следует отметить выдающееся место, занимаемое этапом «построения гипотезы» во всем процессе (или цикле) аналитической работы. Все предварительное планирование работы по выполнению поставленного задания подсознательно основывается на предположениях и догадках, которые имеют отношение к изучаемой проблеме. Фактически без гипотез невозможно даже думать об исследовании какого-либо вопроса. Иногда, составляя перечень этих гипотез и критически оценивая правильность каждой из них, мы обнаруживаем некоторые старые ошибки и находим более успешный метод решения стоящих перед нами задач. Большое количество предположений, выдвигаемых в процессе исследовательской работы, редко подтверждается или выясняется, что некоторые из них содержат серьезные ошибки. Из всех этапов аналитической работы построение гипотезы больше всех связано с процессом чистого мышления. Построение гипотезы практически можно рассматривать как важнейший этап исследовательского цикла, а все остальные основные этапы – как вспомогательные.

Этап 4. Разработка конкретной программы. Разработку конкретной программы деятельности АС следует начать с выработки общей аналитической стратегии. Этот процесс иллюстрируется представленной на рис. 2 диаграммой информационного поля, соответствующей модифицированной схеме И.М. Марти (The Art and Science of Business Intelligence Analysis. Advances in Applied Business Strategy Series, Supplement 2, 1996. – JAI Press, Greenwich, Conn., USA, далее – ASBIA).

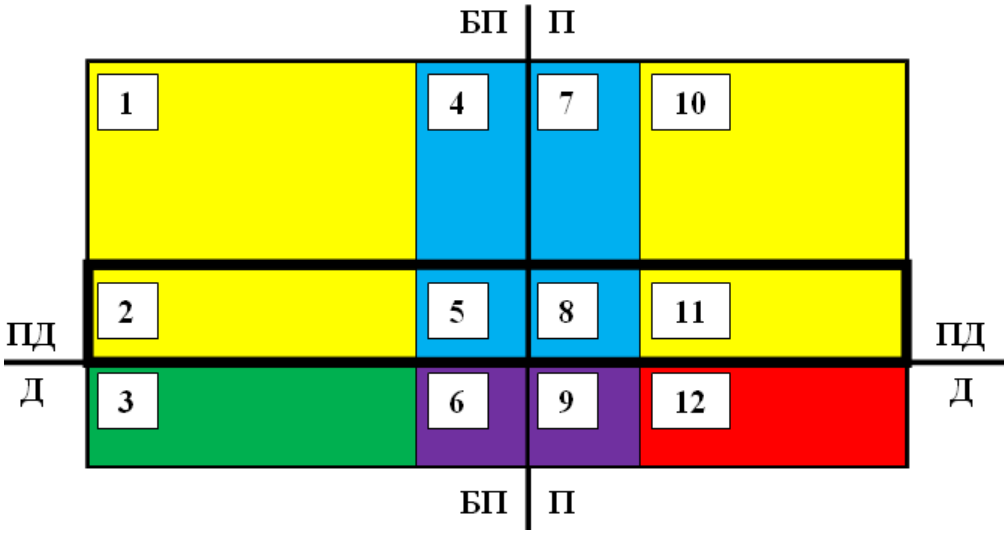


Рис. 2. Упрощенная диаграмма информационного поля

Информационное поле (изображенное в виде заштрихованных секторов) – это совокупность информации, которая уже существует или будет создана до момента принятия решений, поддержку которых должна обеспечить АС.

Зона, лежащая ниже горизонтальной линии ПД-Д (сектора 3, 6, 9, 12), соответствуют *реально доступной информации*, которая уже известна МВУУ или может быть ими получена от подразделений фирмы. Зона, обведенная жирной линией (сектора 2, 5, 8 11) – это *потенциально доступная информация*, та, которая станет доступна МВУУ в процессе нормального функционирования фирмы.

Для облегчения понимания рассматриваемой проблемы вся информация, образующая информационное поле, разделена вертикальной линией БП-П на информацию бесполезную (сектора 1–6) и полезную, т.е. способствующую улучшению качества решений (сектора 7–12). Так, сектор 1 соответствует явно ненужной для фирмы информации, которая к ней никогда и не попадет. Сектор 2 – это информационный шум (например, ненужные рекламные материалы, которые поступят на фирму, непрофильные издания, на которые уже оформлена подписка, будущие результаты неверно сформулированного мониторинга и т.п.). Сектор 3 – это информационный мусор, который хранится на фирме, например, в виде каких-то устаревших отчетов, проектов и прочее).

Сектора 4–9 соответствуют информации, которую хотят получить МВУУ. Видно, что в общем (и типичном) случае МВУУ, не будучи профессионалами в информационной области и действуя в условиях постоянного напряжения и дефицита времени, не в состоянии точно определить, какая информация им действительно необходима. Поэтому часть запрашиваемой ими информации на самом деле бесполезна (ей соответствуют сектора 4–6). Так, МВВУ часто требуют предоставления им максимально полных данных по многочисленным второстепенным вопросам, например, о малозначительных аспектах деятельности конкурентов, поставщиков. Позже выясняется, что они явно не в состоянии изучить и осмыслить представленные им сведения.

Из рис. 2 видно, что без специальных усилий АС МВУУ вполне осознанно получили или получат только ограниченную часть действительно необходимой им информации

(соответствующей секторам 9 и 8). Получить интересующую их информацию из сектора 7 им не позволяет ограниченность информационных ресурсов, а о существовании больших объемов полезной информации, имеющейся даже у них на фирме (сектор 12) и тем более вне ее (сектора 10 и 11) они даже не подозревают. Сектора 10–12 составляют «слепые пятна» информационного поля МВВУ.

Из этого краткого анализа очевидно, что в распоряжении АР имеются несколько путей повышения уровня полезных знаний, которыми обладают МВВУ.

Первое, и во многих случаях самое важное, направление состоит в том, чтобы сократить «слепые пятна» в секторах 11 и 12, т.е. изменить представление МВУУ о факторах, подлежащих учету при принятии решения, и показать, что фирма игнорирует ценную информации, уже имеющуюся в ее распоряжении. В этом и состоит одно из решений задачи по развитию фирмы. Например, АС может показать, что в связи с изменившимися требованиями по утилизации промышленных отходов перед фирмой открывается возможность выгодно реализовать свои старые разработки, которые раньше были признаны экономически неэффективными (это соответствует расширению сектора 9 за счет сектора 12).

Второе направление, заслуживающее самого серьезного внимания, состоит в сборе новой и неожиданной для МВУУ информации в секторе 10, с представлением убедительных доказательств ее ценности (т.е. с расширением за ее счет сектора 7). Так, оперативно полученные данные о новейших технологиях, если фирме удастся их освоить раньше конкурентов, могут открыть фирме дорогу к лидерству в отрасли. И напротив, отставание в этом вопросе способно создать серьезнейшую угрозу для конкурентоспособности продукции фирмы.

Действия АС, направленные на сокращение объема секторов 2 и 5, – это третье направление, ориентированное на повышение эффективности информационной работы за счет сокращения затрат на сбор и обработку бесполезных данных. Освободившиеся за счет этого ресурсы могут быть направлены на решение действительно актуальных аналитических задач.

Таким образом, изучение информационного поля МВВУ позволяет АС понять, какого типа информация требуется лицам, принимающим решения. Это ясное представление требуемого конечного результата дает возможность разработать программу аналитической работы, т.е. четко определить, какого рода исходные данные необходимо собрать и какие именно аналитические методы целесообразно применить для их преобразования в форму, наиболее удобную для МВВУ.

Этап 5. Сбор данных. В зависимости от важности и специфики решаемых аналитических задач, а также от имеющихся в распоряжении АС ресурсов, сбор данных может осуществляться в непрерывном режиме (режиме мониторинга), в пакетном и фокусном режимах.

Наибольший объем данных может быть получен в режиме мониторинга. В то же время осуществление мониторинга связано с наибольшими затратами. Поэтому этот режим эффективен для сбора данных только о важнейших, постоянно действующих факторах внешней среды (политических, экономических и т.п., действий важнейших конкурентов). Фокусный режим соответствует проведению сбора данных отдельно по каждой аналитической задаче. Если ведется параллельная проработка нескольких

задач, требующих для своего решения обращения к одним и тем же информационным источникам, естественно осуществлять сбор данных одновременно по всем этим задачам, т.е. работать в пакетном режиме.

Если МВВУ ясно представляют, какая именно информация им нужна, т.е. именно они являются инициаторами ее поиска, поисковые задачи, как правило, оказываются достаточно четкими и стабильными. В таких случаях (связанных с работой в секторах 7 и 8) имеется возможность использовать стандартные процедуры сбора данных, с применением имеющихся у АС каналов одного или нескольких различных типов. Если фактор времени не является критичным, можно использовать такие процедуры сбора данных, как опросы, интервью, рассылка письменных запросов. Наилучшим методом сбора больших объемов данных в кратчайшие сроки, естественно, является обращение к электронным базам данных.

Для выявления новой, неожиданной и, следовательно, потенциально наиболее ценной информации стандартные поисковые процедуры малопригодны (особенно в отношении данных из сектора 12), поскольку в этом случае нужно «найти то, не знаю, что». Поэтому многие фирмы стараются поощрять творческое отношение своих сотрудников к обнаружению или генерации новых идей и ассоциаций (ASBIA).

Неисчерпаемые возможности для ассоциативного поиска открывают электронные базы данных универсального профиля. Например, фирма, разрабатывающая по заказу крупной приборостроительной фирмы термоконтроллеры для диапазона 20–30 С, может произвести поиск на сочетание слова «регулировка» или его синонимов с любыми поддиапазонами указанного диапазона и неожиданно для себя обнаружить, что ее контроллеры могут найти применение в изделиях типа электроодеял.

Этап 6. Анализ и синтез. Арсенал аналитических методов, применяемых АС, очень широк.

Систематизация исходных данных. Систематизация может проводиться по временному признаку, по исследуемым объектам (например, по фирмам-конкурентам или товарным категориям), по типу действий (например, можно группировать иностранные фирмы по признаку наличия их филиалов или дочерних фирм в том или ином регионе) и т.д. Даже такое простое упорядочение данных может существенно облегчить понимание изучаемой проблемы. Например, анализируя цепь покупок и продаж дочерних фирм крупного концерна, можно сделать важные выводы об изменении его стратегии диверсификации (ASBIA). Объединяя данные о каждой фирме-конкуренте, полученные из множества источников, в интегральные многоаспектные досье фирмы, аналитик может не только выявить их стратегические устремления и применяемые ими конкурентные стратегии, но и проникнуть на более глубокий и стабильный уровень конкурентных преимуществ, т.е. уникальных материальных и, главным образом, интеллектуальных ресурсов, которыми обладает та или иная фирма. Эффективным инструментом для решения этой задачи является комплексный анализ интеллектуального потенциала фирмы с применением патентных источников, научных публикаций, материалов научно-технических отчетов и т.д. (В.Д. Васильев, Б.И Лифляндчик, 1982).

Количественные методы. В эту группу входят, прежде всего, «классические» методы математической статистики и эконометрии (анализ временных рядов, факторный, корреляционый, регрессионый анализ и т.д.). Большое число количественных методов

разработано применительно к задачам финансового анализа, например, с применением различных индикаторов состояния фирмы, основанных на данных ее балансовых отчетов и отчетов о прибылях и убытках.

Важной причиной использования моделей в АС является недоступность значительной части информации, критичной для принятия важных решений: о прибыли, которую приносят конкуренту продажи конкретного товара, об его издержках, связанных с производством этого товара, и т.д. Именно это заставляет АС собирать данные о различных, в отдельности малозначимых действиях конкурентов, в той или иной степени являющихся отражением недоступных искомых переменных.

Ситуация с применением подобных косвенных подходов в практике АС существенно изменилась с появлением возможности работать с профессиональными базами данных. С одной стороны, стало доступным огромное количество годовых отчетов перед акционерами, материалы судебных процессов, обзоры рынков и другие источники, содержащие именно те сведения (например, прямые оценки значимости изобретений, оценки перспективности новых товаров, сведения о прекращении разработок и т.п.), на получение которых не очень надежными косвенными методами приходилось тратить массу усилий и времени. С другой стороны, возможности применения косвенных методов также значительно расширились, поскольку появилась возможность отслеживать почти в реальном времени такие действия интересующих фирм, как смена руководства, покупка или продажа лицензий, торговых знаков, дочерних фирм, заключение стратегических союзов, строительство новых предприятий и т.д.

Проблемы использования математических моделей. С ростом объемов количественных данных, доступных для анализа, а также с быстрым ростом вычислительных мощностей и совершенствованием программ обработки данных количественные методы будут становиться все более популярными в работе АС. Следует, однако, помнить и о серьезных проблемах, связанных с не всегда продуманным использованием количественных моделей. В целом ряде случаев использование таких моделей связано с принятием многочисленных допущений, которые не соответствуют реальным условиям применения моделей. Например, для оценки полезности товара обычно применяются линейные аддитивные модели, полностью аналогичные моделям, разработанным ранее в СССР для оценивания уровня качества. Однако очевидно, что оценка того или иного атрибута товара (его частная полезность) нелинейным образом зависит от уровня присутствия этого атрибута. Например, удвоение разрешающей способности принтера, предназначенного для печатания простых текстовых документов, со 150 до 300 dpi может рассматриваться как значительное улучшение. Переход от 300 до 600 dpi не окажет заметного влияния на оценку принтера средним потребителем, тогда как дальнейшее улучшение вообще не имеет для него практического смысла.

Главное ограничение применимости количественных моделей в АС состоит в следующем. Конечной целью любого анализа, проводимого АС, в том числе с применением количественных моделей, является синтез, т.е. создание целостной картины проблемной ситуации в будущем (например, возникновение угрозы со стороны конкурентов), которую нужно разрешить путем принятия и осуществления соответствующих решений. Использование при этом результатов количественного моделирования всегда означает экстраполяцию прошлого в будущее, т.е. принятие

(хотя часто и неосознанное) гипотезы о сохранении неизменными тех факторов, которые определили количественные характеристики используемой модели. Другими словами, обычные математические модели не могут предсказать и учесть внезапные резкие изменения внешней среды, например, принятие новых законов или постановлений, появление товаров нового типа, резкого изменения ситуации в отношении ликвидации задолженности по зарплате и т.д.

Чем более динамичной становится внешняя среда, тем более иллюзорной становится точность расчетов объемов будущих продаж, а, следовательно, будущих прибылей и/или убытков, рассчитанных с применением самых мощных финансовых моделей. Такое крупное потрясение, как нефтяной кризис 70-х годов, опрокинуло большинство количественных прогнозов. В меньших масштабах аналогичная ситуация повторилась и в связи с финансовым кризисом осени 1997 г.

«Творческие» методы. Наиболее известным в этой группе является «метод сценариев», который ориентирован на то, чтобы выявить и подчеркнуть принципиальную неопределенность будущего в условиях турбулентной внешней среды. Согласно этому методу разрабатываются несколько вариантов будущего развития событий, которые обычно включают как минимум пессимистический, оптимистический и наиболее вероятный варианты. Метод сценариев облегчает интеграцию различных данных, полученных как качественными, так и количественными методами, он хорошо совместим также с методами теории игр, разработанными применительно к анализу конкурентных ситуаций (ASBIA). Одна из главных задач метода сценариев – выявить «ключевые» факторы, от которых будет зависеть развитие событий по тому или иному сценарию. Разработав варианты своей стратегии и тактики применительно к основным сценариям и осуществляя мониторинг «ключевых» факторов, фирма значительно расширяет свои возможности быстрого реагирования на резкие изменения внешней среды.

Компьютеризация аналитической обработки данных. Как уже отмечалось выше, АС должна быть способна извлечь полезные сведения практически из любого документа, имеющего хотя бы самое отдаленное отношение к бизнесу. С учетом взрывного роста количества электронных документов при соответствующем развитии средств коммуникации для АС открывается доступ буквально к миллионам документов, которая она в принципе может использовать в своей аналитической работе. Поэтому неудивительно, что одной из наиболее быстро развивающейся областей информационных технологий является программное обеспечение обработки данных для целей АС. Например, компания LEXIS-NEXIS разработала специальные информационный продукты Tracker и InfoTailor, которые сканируют более 6 тысяч информационных источников, отбирают по предварительно разработанной стратегии поиска только те статьи или документы, которые представляют интерес для заказчика. Отобранная информация ежедневно к 9 утра доставляется заказчику на его собственный WWW сайт. Стоимость таких информационных продуктов состовляет менее $200 в месяц. В качестве еще одной иллюстрации упомянем аналитические программные продукты, предлагаемые американской фирмой Manning & Napier Information Services (Competitive Intelligence Tools. Business Wire May 15, 1997). Программа DR-LINK (уже используемая рядом фирм, включая корпорацию Кодак) служит для сканирования новостных сообщений с целью извлечения из них сведений прогнозного и аналитического характера, оценок, концепций и других важных компонентов, которые трудно или невозможно выделить с помощью традиционных

средств информационного поиска.

Программа MAPIT способна прочесть, проанализировать и провести сравнение (в том числе с применением наглядных графических методов) тысяч патентов в течение всего нескольких часов, группируя патенты, например, по признаку близости технологий. Одно из эффектных средств MAPIT – очень наглядное графическое представление взаимодополнительных или конфликтующих патентных формул. Очевидно, что такой анализ способен многократно снизить неопределенность оценки патентно-лицензионной ситуации, которая существенно связывает свободу действий очень многих фирм, особенно в высокотехнологичных областях.

Этап 7. Выводы. На этом этапе производятся исследования, необходимые для доказательства или опровержения рабочих гипотез и формулируются окончательные выводы, являющиеся душой почти любого аналитического документа. Для того чтобы аналитическая информация, поступающая от АС к МВУУ, оказала влияние на принимаемые ими решения, она должна быть убедительной. Ограничимся несколькими простыми рекомендациями, которые нужно в связи с этим учитывать при представлении результатов работы.

1. Чтобы быть убедительным, аналитический документ должен, прежде всего, вызвать интерес МВУУ благодаря эффектной подаче материала, логичности, понятности, информационной насыщенности.

2. Убедительный документ, как правило, включает следующие основные компоненты:

- ясную формулировку цели, ради которой он написан (применительно к АС типичной целью является аналитическое обеспечение управляющего решения);

- изложение результатов анализа и синтеза информации (например, ухудшение конкурентного положения фирмы в связи с падением спроса на ее продукцию);

- возможные действия со стороны фирмы и их вероятные последствия;

- оценка надежности сделанных выводов и рекомендаций, а также возможных последствий их ограниченной надежности.

3. Эффективность материалов АС может быть значительно повышена за счет их индивидуализации в отношении управляющего решения, которое они обеспечивают, и конкретного МВУУ, которому они адресованы. Эта индивидуализация касается как момента представления, так и формы и объема представляемых материалов.

4. Объем представляемых материалов практически всегда ограничивается возможностями их восприятия МВУУ, которые постоянно перегружены. Вместе с тем, чем более сложное и важное решение предстоит принять, тем больший объем информации будет готов изучить МВУУ.

5. Оценка надежности выводов должна складываться из оценок полноты и надежности исходных данных и эффективности методов их преобразования в аналитическую информацию. Как было показано выше, надежность преобразования существенно снижается при использовании аналитических методов, использующих нереалистичные допущения (это относится ко многим математическим моделям, особенно линейным) или способных использовать только часть доступной информации. Существенное повышение надежности может быть во многих случаях

достигнуто параллельным применением нескольких альтернативных методов анализа.

Чем менее надежна представляемая информация, тем большее внимание должно быть уделено анализу возможных последствий принятия неоптимального или ошибочного решения.

Этап 8. Изложение. Составление документа, завершающее работу. Составитель аналитического документа должен не только ясно представлять себе то, о чем он пишет, но и уметь выразить свои мысли в ясной форме. Необходимо указывать степень достоверности каждого утверждения. Работа, проделанная на каждом этапе, считается предварительной, и могут быть внесены изменения в зависимости от новых данных, полученных по мере продолжения исследования на последующих этапах. Например, сбор фактов нельзя провести сразу и закончить в один прием. После того как собрана часть фактов, их истолкование, несомненно, покажет, по каким вопросам требуется собрать дополнительные факты, и тем самым даст направление последующей исследовательской работе. Точно так же дело обстоит и на других этапах. Например, общий план работы является в момент его разработки предварительным. Мы должны быть готовы принять его и в равной мере должны быть готовы возвращаться назад и вносить изменения в предварительный план каждый раз, когда в свете новых данных в этом возникнет необходимость. Применяя метод обратной последовательности этапов, мы расширяем свои знания по изучаемому вопросу в соответствии с принципом сложных процентов, получая проценты на проценты.

В материалах, с которыми работает аналитическая служба (АС), различаются:

- данные из (от) источников;

- разрабатываемые разведывательные документы;

- организационно-распорядительные документы;

- справочники, досье, архивы.

Соответственно выделяются технологии: работы с данными источников; разработки документов; делопроизводства; информационного обеспечения.

Возможные режимы работы аналитика:

1) решение конкретных задач: в нормальном, ускоренном, экстремальном темпе;

2) поддержание интеллектуальных навыков (чтение книг и периодики), слежение за текущей ситуацией, общение с различными людьми;

3) формирование обобщенных представлений и развитие профессиональных технологий.

В процессе разведывательного анализа выявляются: состояния различных феноменов; представления различных субъектов об этих феноменах; намерения различных субъектов; имитации различными субъектами состояний, представлений, намерений. Хант Ч. и Зартарьян В. предлагают разделять совокупность исследуемых АС феноменов по степени важности на следующие три сферы (рис. 3).

Рис. 3. Степени важности исследуемых феноменов

Работа аналитической службы включает в себя следующие компоненты:

1. Добывание:

- разовое изучение различных феноменов;

- мониторинг текущих состояний различных феноменов.

2. Анализ:

- текущих (быстро изменяющихся) характеристик субъектов, объектов;

- базовых (медленно изменяющихся) характеристик субъектов, объектов;

- устройства и состояния субъектов, объектов;

- приемов деятельности субъектов;

- процессов, имеющих место в объектах или вовлекающих в себя объекты;

- обобщенных представлений субъектов;

- стратегий, прогнозов, планов субъектов;

- возможностей (мощностей, резервов, запасов, потенциалов) субъектов;

- способов приведения субъектов, объектов к тому или иному состоянию.

3. Реконструирование:

- выяснение причин того или иного процесса, события, качества;

- расследование и объяснение прошлых событий.

4. Прогнозирование: оперативное; стратегическое.

5. Оценивание субъекта, объекта, события, процесса: выяснение степени полезности, вредности, опасности, важности.

6. Планирование: оперативное; стратегическое.

7. Теоретизирование: разработка теорий, идеологий, доктрин, стратегий.

Исследование, анализ, прогнозирование могут быть формальными и неформальными. Формальные – осуществляемые посредством действий с данными. Они более или менее легко алгоритмизируются, то есть выражаются в виде исчерпывающе описанных процедур. Неформальные – осуществляемые посредством действий с мысленными представлениями. Детальное регулирование их посредством предписывания четких процедур мешает достижению высококачественых результатов. Формальные процедуры работы с данными становятся применимыми после формализации сведений, то есть после представления их в виде данных на некотором простом языке. Возможное содержание формального анализа:

- выявление наибольших, наименьших, средних значений; ранжирование (по одному признаку или по нескольким взвешенным признакам).

- выявление сходства, различия;

- фильтрование (отбор по некоторым критериям);

- классифицирование;

- выявление степени корреляции;

- проверка статистических гипотез.

Аналитическое обеспечение важных управляющих решений, которые принимают менеджеры высшего уровня управления, – это один из инструментов менеджмента, роль которого в условиях конкурентной борьбы явно недооценивается многими российскими руководителями и предпринимателями. Высокая эффективность аналитической службы может быть достигнута лишь в условиях высокого доверия к ней со стороны руководства фирмы. Такое доверие может быть оправдано только при правильном подборе руководителя аналитической службы и обеспечения ее необходимыми ресурсами для реализации различных вариантов сбора и аналитической обработки исходных данных. Главное направление развития аналитической службы – широкое использование электронной документации, особенно из многочисленных, и, в первую очередь, крупных, электронных баз данных. Сложности глубокой переработки больших массивов электронных документов делают актуальных применение специальных аналитических программ и/или обращение к специализированным фирмам, оказывающим услуги в области аналитического обеспечения.

Глава 3. Работа с источниками информации

3.1. Информация – основа успеха

Связь информации с областью деятельности. Представьте себе сотни элементов головоломки, сваленные в беспорядке в сундук на чердаке. Это позволит вам получить довольно точное представление о «сырой» информации, которая осаждает вас со всех сторон. Речь идет о груде хлама, не представляющего в целом интереса, в котором, однако, скрываются некоторые ценные сведения. Изолированная информация не позволяет составить сколько-нибудь полное представление о каком-либо событии, точно так же, как отдельный элемент загадочной картинки не позволит судить о ее полном содержании, как бы вы его не вертели у себя перед глазами. Вера в то, что путем прибавления информации к информации вы неизбежно поймете суть дела, подобна вере в то, что, набирая побольше элементов из груды перепутанных частей разных головоломок, вы ускорите восстановление загадочной картинки. Иными словами, ваше терпение может истощиться задолго до того, как вы найдете два совместных элемента картинки, т.е. задолго до того, как вам удастся объединить отдельные информационные сообщения в единое целое.

Так, события, происходящие на государственном уровне, представляются все менее и менее понятными по мере увеличения числа репортажей, интервью, обсуждений за круглым столом и т.д. В январе 1990 г. в газете «International Herald Tribune» была опубликована статья под заголовком: «США затоплены потоком информации из СССР». В этой статье сообщалось, что после 45-летнего периода информационного голода аналитики американского правительства буквально тонут в информации, поступающей из СССР после выхода на сцену М.С. Горбачева. И тем не менее, вся эта информация не позволила предвидеть скорость и размах событий в Восточной Европе и в республиках СССР.

Несмотря на свой большой объем и разнообразие, этот поток информации ничего в конечном счете не прояснил. Он даже не позволил экспертам ответить на самые простые вопросы, такие, как причины выхода в отставку ряда высших должностных лиц. Такие ничтожные результаты вынудили руководителей американских разведывательных служб заявить: «Мы нуждаемся в новых методах».

Если опыт показывает, что информация и понимание сути дела не являются синонимичными понятиями, то это означает, по-видимому, что постановка проблемы оказалась неправильной: считается, что информация – это объект, который существует в абсолюте, идентичный для всех, а исходить нужно, очевидно, из того, что речь идет о конструкции, которую каждый строит сам для себя в соответствии со своими потребностями.

Подлинная информация существует лишь в том случае, если предварительно имеется намерение (замысел), цель, проект. Намерение предопределяет отношение, более или менее осознанное, к анализу окружающей действительности, что в свою очередь выражается в пробуждении внимания, в результате чего единственное слово, объект или событие, имеющее к нам отношение, вылавливается из неупорядоченного множества сигналов.

В конечном счете, истинная информация является результатом взаимодействия пары намерение – внимание, а все остальное является только шумовым фоном. Представьте себе, что вы находитесь в незнакомом городе и вам нужно сесть в поезд. К счастью вы встретили полицейского, который укажет вам путь. Здравствуйте, как пройти на вокзал? Для этого вам потребуется не более 5 минут. Идите по этой улице до перекрестка. На перекрестке повернете направо на бульвар Виктора Гюго. Затем у памятника, большой статуи посредине бульвара, слева начинается вокзальная улица. Вокзал находится в конце этой улицы, вы его увидите. Спасибо.

Получив эту ценную информацию, вы отправляетесь в путь. Как вам было указано, на первом перекрестке вы поворачиваете направо и проверяете, действительно ли вы находитесь на бульваре Виктора Гюго. С этого момента у вас на уме только одна мысль: отыскать памятник поэту, чтобы не пройти мимо вокзальной улицы. Бульвар может быть обсажен деревьями, вы можете проходить мимо универмага, все это не представляет для вас ни малейшего интереса (если вы не собираетесь делать покупки). Все ваше внимание сконцентрировано на середине улицы до появления памятника. Это и есть та информация, которой вам недоставало для достижения цели, то есть вокзала.

Отыщите у себя в памяти случаи, когда одно слово, образ, имя привлекало ваше внимание. Попытайтесь восстановить причину, т.е. выяснить намерения, неявный запрос, которые обусловили такое ваше внимание. Если, как было предложено, отправной точкой считать выполняемое действие, преследуемую цель, а не окружающий нас псевдоинформационный шум, то перспектива коренным образом изменяется. Становится возможным создание эффективного метода сбора и обработки информации без ненужных потерь времени, путаницы и риска утонуть, который обеспечит получение всех необходимых и только необходимых сведений. Информация не имеет смысла без связи с действием. Информация = намерение + внимание.

С общей точки зрения для получения надлежащей информации необходимо тщательно выбрать базы для наблюдения, которые предопределяются насущными потребностями, т.е., в свою очередь предопределяются поставленными целями. Так, птичье пение не несет никакой информации для Жана Мартена, однако оно является ценной информацией для охотника. И, напротив, знание положения по отношению к солнцу совершенно бесполезно для поиска дичи, но крайне необходимо для Жана Мартена в поисках его пути домой. В этом и заключаются так называемые «3B» (buts – besoins – bases), служащие фундаментом для построения информации: цели – потребности – базы. Цели связаны друг с другом в иерархическую структуру. Каждая цель предопределяется целью высшего порядка, оставаясь при этом автономной, по характеру своих потребностей и баз для наблюдения. Так, после стратегической цели определение направления следует тактическая цель выбор наилучшей дороги и. наконец, оперативная цель продвигаться вперед по выбранной дороге.

Каждой из этих целей соответствуют различные потребности в информации и, следовательно, разные базы для наблюдения. Это является справедливым для любой организации и, в частности, для предприятий, где следует различать стратегический уровень (строительство фабрики, внедрение новой технологии, запуск в производство новой продукции т.п.) и тактический уровень, (выбор площадки для строительства фабрики, закупка лицензии или разработка новой технологии собственными силами

и т.д.). Правильное определение целей на каждом уровне позволяет правильно определить потребности в информации и, одновременно, базы для наблюдения.

Информация для стратегических решений. Стратегические решения прямо влияют на судьбу предприятия, на его развитие и жизнеспособность. Окружающий мир постоянно изменяется. Скорость этих перемен постоянно увеличивается. Поэтому число стратегических решений постоянно растет, их последствия все сложнее и сложнее прогнозировать, а цена ошибки постоянно повышается. Этим и определяется значение стратегической информации. Она является обязательным сырьем для выработки любого решения, без чего самые прекрасные планы останутся простым самообманом и неизбежно обречены на неудачи.

Легко понять, что без качественной информации невозможно принять правильное решение, однако гораздо труднее руководствоваться этим выводом на практике. Как собрать всю информацию, которая может оказаться полезной для принятия будущих решений, если еще неизвестен их точный характер, и при этом не утонуть в информационном шуме?

Решение, как мы теперь знаем, заключается в поэтапном подходе в соответствии с методом «ЗВ»: работа должна начинаться с определения целей, которые предопределят потребности в информации, а затем и базы для наблюдения. Начинать работу с определения баз для наблюдения или, что еще хуже, хотя и часто встречается, с поиска источников – значит совершить роковую ошибку. Это, конечно, позволит собрать определенный объем данных, однако большинство из них окажутся бесполезными, а немногие полезные данные затеряются в массе ненужной информации. Служба информации окажется постепенно оттесненной на задворки предприятия, подальше от дирекции, а ее сотрудники постепенно превратятся в озлобленных замкнутых функционеров. Одним словом, в этом случае мы получим антитезу эффективной службы информации, которая должна находиться в постоянном и тесном контакте с внешним миром и с инстанциями, уполномоченными принимать решения. Метод «ЗВ» позволяет избежать таких ошибок, которые ведут к сбору подряд любой информации.

Информация о подготовке военного переворота против главы государства является, несомненно, чрезвычайно важной для правительства, но не представляет ни малейшего интереса для руководителя фирмы, пытающейся проникнуть на внутренний рынок США. Напомним, что абсолютной информации не существует, а есть только информация по отношению к намерениям лица, которое опрашивает внешний мир для того, чтобы действовать в этом мире и воздействовать на этот мир. То, что для одного является информацией, для другого является просто шумом. Однако в один прекрасный день этот шум может превратиться в информацию. Таким образом, не существует двух похожих систем. Каждая система должна быть сделана по мерке. Для того чтобы это было понятней, рассмотрим, пример фирмы «Trident».

Стратегические цели. Мишель Билаль, президент фирмы «Trident» стремится к дальнейшему развитию деятельности фирмы в области производства спортивной одежды и обуви, которое связано с передовыми технологиями и высокой прибавочной стоимостью. У него нет ни малейшего желания заняться производством спортивного инвентаря (теннисных ракеток, лыж и тл.), которое он считает совершенно отдельной областью профессиональной деятельности. Следует отметить, что речь идет только о мнении нынешнего директора фирмы «Trident». Другие лица или другие фирмы могут

иметь по этому поводу иное мнение. Однако это его мнение предопределит все последующие действия. Поэтому очень важно не жалеть времени на обдумывание и размышления.

Стратегические потребности. Они включают в себя все, что может оказать долгосрочное влияние на деятельность предприятия. Для фирмы «Trident», учитывая поставленные стратегические цели, речь идет о таких областях, как развитие спорта и физкультуры, технологий разработки и производства одежды и обуви, изменение вкусов публики. Кроме того, фирма «Trident» не является единственным действующим лицом на этой сцене. Ее позиции могут быть поставлены под сомнение ее действующими или Потенциальными конкурентами. В число потенциальных конкурентов входят как крупные швейные предприятия, способные расширить ассортимент своей традиционной Продукции за счет спортивной одежды, так и производители оборудования, которые хотели бы расширить ассортимент услуг, которые они предоставляют своей клиентуре.

И, наконец, следует учитывать непредвиденные случайности, связанные с изменениями моды или с климатическими и погодными условиями, которые имеют большое значение в области спорта, и найти противоядие. Так, стоит задать себе вопрос: каким еще потребностям может соответствовать продукция фирмы «Trident» (напомним случай с альпинистской ветровкой, покупаемой охотниками?). Или какую другую одежду может выпускать фирма «Trident» благодаря своему «ноу-хау».

Такой перечень потребностей в стратегической информации должен быть предельно полным. В этом случае лучше перебрать, чем что-то упустить. Очень часто события, имеющие очень большое значение для судьбы предприятия, происходят за пределами ее непосредственной области деятельности и влияния. Обследование 22 предприятий из 7 различных отраслей промышленности, проведенное Купером и Шенделем, показало: более половины всех технологических новинок появились за пределами их традиционной области деятельности – шариковая авторучка, фотокопирование, кварцевые часы и т.д.

Стратегические базы. На основании выявленных потребностей следует составить картотеку направлений для наблюдения. Пример фирмы «Trident» показывает, что определение потребностей является, по всей видимости, наиболее сложным этапом метода «ЗВ». Действительно, почему нельзя перейти непосредственно от целей к построению баз для наблюдения? Цели являются выражением желаний: они определяют желаемое. Что касается баз, то они представляют окружающий мир и выражают необходимость. Между собой и окружающим миром, между желаемым и необходимым следует перебросить мост – мост возможного. Именно этой цели и служит промежуточный этап определения потребностей. Для облегчения этой работы представляется рациональным разделить сферу действий на три области:

- непосредственная сфера действий включает в себя все, что находится в прямой связи с деятельностью фирмы – от поставщиков до потребителей, включая конкурентов и вопросы технологии;

- сфера влияния включает в себя все, что может оказать влияние на действия, осуществляемые в рамках предыдущей сферы. Так, например, фирма «Trident» может подвергнуться влиянию со стороны производителей лыж, динамики моды и вкусов населения, химической промышленности (разработка новых синтетических тканей и

пластмасс), политической ситуации в других странах;

- сфера интересов включает в себя области деятельности, которыми фирма пока не занимается, но может заняться в будущем, а также те области деятельности, которые могут вторгнуться в основную сферу деятельности фирмы. В нашем примере сфера интересов включает в себя потенциальных конкурентов, спецодежду и т.д.

Польза такого деления заключается в том, что оно вынуждает обратить свое внимание за пределы обычной сферы действий, то есть туда, откуда обычно исходят наиболее крупные благоприятные возможности и самые большие опасности. Так, производители часов традиционного типа были сметены с рынка, так как они не обратили внимания на быстрое развитие электроники, которая не имеет ничего общего с точной механикой. Если автомобилестроительное предприятие следит за деятельностью своих конкурентов, то оно, конечно же, должно интересоваться фирмами «BMW», «Mersedes» и т.д. Но оно должно также держать в поле своего зрения предприятия, занимающиеся судостроением, строительством плавательных бассейнов и т.д.

Чем больше поставленные цели удалены во времени, тем шире должно быть поле зрения, тем пространнее должна быть сфера интересов. Особое значение это имеет на стратегическом уровне. В то же время, на тактическом и оперативном уровне можно ограничиться двумя первыми сферами, то есть непосредственной сферой деятельности и сферой влияния.

Информация для тактических решений. Тактические цели. Заблудившийся человек знает куда он желает прийти (стратегическое решение), а теперь он должен решить по какой дороге идти (тактическое решение). Тактическая цель заключается в выборе наилучшего средства достижения стратегической цели и в контроле неизменности условий, которые предопределили этот выбор.

Предположим, что Мишель Билаль президент фирмы «Trident», принял стратегическое решение о строительстве фабрики в одной из стран с дешевой рабочей силой. На тактическом уровне первая проблема будет заключаться в выборе наиболее подходящей страны. Затем следует проследить за неизменностью условий, предопределивших этот выбор. Иными словами, следует проследить за тем, чтобы не возникли непредвиденные препятствия. Так, весь проект окажется бесполезным, если ЕЭС введет новые ограничения на импорт текстиля.

Тактические потребности. Что требуется для правильного выбора дороги? Представим себе, что заблудившийся человек располагает картой, на которой указаны две дороги, ведущие к намеченной им цели. Первая дорога – горная, она короткая, но извилистая и крутая. Вторая дорога проходит по равнине в обход гор. Эта вторая дорога более длинная, но, несомненно, и более легкая. Таким образом, может сложиться впечатление, что карта содержит достаточную информацию. На самом же деле при выборе дороги необходимо учитывать и другие факторы, о которых карта умалчивает. Так, зимой горная дорога из-за снега может оказаться непроходимой. А летом у этой же самой дороги, по сравнению с равнинной, гораздо больше шансов оказаться перерезанной разливающимися горными потоками. Эти факторы относятся к числу переменных и не могут быть указаны на карте. Однако их следует знать достаточно заблаговременно с тем, чтобы вынужденный поиск обходных путей не свел на нет все преимущества правильного стратегического решения.

Из приведенного примера следует, что необходимо различать постоянную окружающую среду (горы, овраги, болота и т.д.) и переменную окружающую среду (оползни, разрушение моста, разлив реки и т.д.). Для правильного выбора дороги необходимо учитывать как первое, так и второе. Следует отметить, что это различие связано с временной шкалой действий. Поэтому оно не имеет большого смысла на стратегическом и оперативном уровне, где им можно пренебречь. В то же время на тактическом уровне это различие играет очень важную роль и предохраняет два типа потребностей.

Потребности первого типа. Для правильного выбора необходимо знать общие характеристики каждой из дорог. Что касается нашего примера, то есть проблемы размещения фабрики фирмы «Trident» в одной из зарубежных стран, то в этом случае необходимо определить общие характеристики определенного числа таких стран, то есть составить некое подобие карты.

Потребности второго типа Необходимо постоянно наблюдать за состоянием окружающей среды для своевременного выявления всех препятствий, которые могут явиться причиной значительных отклонений от намеченного пути. Это означает, что фирма «Trident» должна внимательно следить за новостями в области законодательства, регламентации, транспорта и т.д.

Эти два типа потребностей настолько различны, что соответствующие им базы практически не имеют ничего общего друг с другом. В первом случае создаются и уничтожаются базы для информации, собираемой «по запросу»: каждый раз, когда появляется новая дорога, предпринимается попытка максимально полного ознакомления с ее характеристиками для принятия решения о том, стоит ли по ней идти. Во втором случае ведется всеобъемлющее наблюдение окружающей среды, так как неизвестно откуда может прийти опасность. Тактические базы первого типа: «по запросу».

Приведем несколько примеров баз, относящихся к новым дорогам, которые фирме «Trident» может быть придется исследовать.

Запуск в производство новой продукции, например, защитной одежды для работы с опасными химическими продуктами. Какие изделия в настоящее время конкурируют на рынке? Есть ли объявления конкурентов о скором выпуске новой продукции этого типа? Над чем работают проектные и конструкторские бюро конкурентов? В состоянии ли конкуренты быстро реагировать? Может ли кто-нибудь заблокировать каналы сбыта? Гарантировано ли снабжение сырьем? Является ли законодательство благоприятным? И если нет, то можно ли внести в него изменения?

Наращивание производственных мощностей. Представим себе, что в текущем году имеет место очень высокий спрос на теннисную обувь – следует ли увеличивать производственные мощности? Для ответа на этот вопрос необходимо выяснить следующее.

Является ли бум краткосрочным или долговременным, то есть идет ли речь о временной преходящей моде (например, звезда эстрады косит теннисные туфли фирмы «Trident» и ее поклонники бросились покупать такую же обувь) или о более глубокой тенденции типа, если вспомнить популярный в свое время лозунг, «жизнь слишком коротка для того, чтобы одеваться угрюмо»?

Если бум носит всеобщий характер и затрагивает всех производителей, то в этом случае все они попытаются увеличить производство и даже могут иметь место попытки новых конкурентов проникнуть на этот рынок. Существует опасность оказаться вскоре с избытком производственных мощностей. Каковы будут тогда затраты? Могут ли вновь созданные мощности после не дорогостоящей переналадки использоваться для производства другой продукции? И если нет, то каковы тогда будут потери?

Развитие технологии производства. Может ли быть наращивание объема производства обеспечено за счет повышения производительности труда? Строительство фабрики в одной из зарубежных стран.

Политическая информация (стабильность режима, возможность вывоза прибыли, уровень коррупции и т.д.).

Социально-кульгурная информация (наличие и качество рабочей силы, отношение к иностранцам, профсоюзная активность и т.д.). Экономическая информация (стоимость земли и строительных работ, возможность получения субсидий, налоговая система и т.д.). Тактические базы второго типа: «всеобъемлющее наблюдение окружающей среды».

Эти базы включают в себя все факторы окружающей среды, изменение которых может оказать среднесрочное воздействие на деятельность предприятия. Прежде всего, речь идет об опасностях рынка и, в частности, об определенных действиях конкурентов. Таким образом, небольшой перечень критериев, учитываемых на стратегическом уровне, удлиняется на тактическом:

- основные области деятельности и виды продукции (нынешние и будущие);

- зоны и территории деятельности;

- производственные мощности и способ производства;

- патентная и лицензионная активность.

Естественно, тактические базы и учитываемые параметры изменяются в зависимости от политической линии, намеченной руководством. Рассмотрим пример, в котором параметр «зоны и территории деятельности» играет особо важную роль. Так, в 1975 г. фирма «Bic» выбросила на европейский рынок бритву одноразового пользования, что вызвало подозрение со стороны гигантской американской фирмы «Gilletti». Угроза подтвердилась, когда в начале 1976 г. фирма «Bic» вторглась на рынок Канады. Следует отметить, что Канада часто служит для европейских и азиатских фирм дверью для проникновения на внутренний рынок США. Поэтому фирма «Gilletti» поспешно выбросила на рынок свою собственную модель бритвы одноразового пользования. Когда фирма «Bic» попыталась выйти на рынок США то оказалось, что он уже занят.

Не следует, однако, думать, что учитываемые на этом уровне переменные параметры, имеют отношение только к маркетингу. Здесь необходимо обязательно учитывать все факторы окружающей среды, оказывающие среднесрочное воздействие на деятельность фирмы. Речь, например, идет о следующем. Законодательство: действующее, готовящееся, лоббистские группировки и т.д. Или введение в 1992 г. новых стандартов на загрязнение окружающей среды автомобильным транспортом. Снабжение: находится ли деятельность предприятия в зависимости от поставок

сырья? Если да, то в чем заключается суть проблемы?

Социальная среда. Политические, экономические и социальные события в странах, где фирма имеет интересы.

Информация для решения оперативных вопросов. Оперативные цели. На этом уровне стратегическая цель уже определена, путь ее достижения выбран. Теперь необходимо обеспечить продвижение вперед в наилучших условиях, избегая последних мелких препятствий и по возможности сокращая путь.

Оперативные потребности. Речь идет о благоприятных возможностях (выявление более выгодного поставщика, подхода к крупному клиенту своего конкурента и т.д.) или об угрозах (банкротство субподрядчика, масштабная рекламная кампания конкурента и т.п.). Во всех случаях требуется свежая, точная, надежная и целенаправленная информация, так как речь идет о максимально быстром реагировании, то есть о реагировании без малейших промедлений и без импровизации: благоприятные возможности, как правило, не повторяются дважды, а угрозы, если их вовремя не предотвратить, могут оказаться гибельными.

Предположим, что поставщик начал неожиданно испытывать трудности с выполнением заказов. Что это означает? Конкурент взял поставщика под свой контроль и теперь блокирует снабжение или поставщик испытывает реальные трудности? В последнем случае речь даже может идти о благоприятной возможности покупки предприятия-поставщика. Оба этих прямо противоположных варианта являются одинаково правдоподобными. Этим обусловливается потребность в качественной информации. Такая информация может быть получена только в результате большой и длительной работы, которая позволит определить направления наблюдений, выбрать самые лучшие источники и разработать эффективные процедуры передачи информации. Так, если через своего банкира удается заблаговременно узнать о резком повышении активности и проявлениях беспокойства среди акционеров фирмы-поставщика, то это будет очень ценным указанием, которое позволит принять соответствующие меры.

Оперативные базы. Речь идет о ближайшем окружении фирмы, за которым необходимо следить с повышенным вниманием. Сюда, естественно, входят конкуренты и, главным образом, их коммерческая политика: ассортимент продукции, цены, рекламные кампании и т.д. Не следует также забывать о других не менее жизненно важных направлениях наблюдения: поставщики, клиенты, система торговли, субподрядчики и многочисленные другие объекты наблюдения, определяемые с учетом специфических потребностей каждого конкретного случая.

На этой стадии знакомства с нашей книгой у вас может сложиться впечатление, что работа по систематическому поиску информации является чрезвычайно сложной и что, если дело и дальше пойдет такими же темпами, то вы вскоре утонете. Не следует заблуждаться. В действительности ваше впечатление связано в основном с новизной этой проблемы, а не с самой проблемой. Вспомните, как вы учились езде на велосипеде. При взгляде со стороны езда на велосипеде представлялась делом простым, но стоило вам сесть в седло и, вы себя почувствовали потерянным. Вам потребовалось одновременно учиться работать педалями, рулить, сохранять равновесие, следить за дорогой. Однако в результате тренировок и накопления опыта все эти действия стали для вас настолько привычными, что теперь вы с удовольствием

катаетесь на велосипеде, не особенно задумываясь над тем, как вы это делаете. Точно так же обстоит дело и с поиском информации.

Совершенно естественно, что вначале вы почувствуете себя перегруженным. Нет ничего ненормального в том, что вначале вы будете совершать ошибки, принимая необоснованные слухи за подлинную информацию. Лишь в процессе поиска информации можно научиться собирать ее. При использовании метода «ЗВ» окружающий пейзаж вскоре становится привычным, сфера действия – картографированной, а вся поисковая работа становится очень простой и сводится к выявлению изменений в пейзаже и несовпадений с картой.

Обучение должно осуществляться последовательно и поэтапно по направлению от ближайшего окружения до наиболее удаленных областей наблюдения. Так, при езде на велосипеде можно любоваться горным массивом лишь тогда, когда вы уверены в дороге, по которой едете.

Усвоив излагаемый метод, вы вскоре окажетесь в состоянии распознавать полезную информацию с первого взгляда. Уйдут в прошлое растерянность и путаница, риск утонуть или упустить ключевую информацию. Качественная информация позволит вам получить преимущество над теми, кто все еще продолжает барахтаться в океане информационного шума.

Картотека наблюдений. В предыдущих разделах мы рассмотрели, как в соответствии с принимаемыми решениями определяются потребности в информации и базы для наблюдения. При этом следует отметить, что отдельные базы для наблюдения объединяются
в определенные группы. Так, наблюдение за деятельностью конкурентов является необходимым независимо от типа принимаемого оперативного, тактического или стратегического решения.

Кроме того, собранная информация может послужить для выработки решений такого типа, для которого она первоначально не была предназначена. Так, фирма тщательно собирает информацию о колебаниях цен на продукцию своего главного конкурента с целью определения своего потенциала сбыта по отношению к этому конкуренту. Но, в один прекрасный момент вся информация о колебаниях цен конкурента была подвергнута углубленному анализу, который позволил выявить коренное изменение его коммерческой политики. Она переориентировалась на мелкосерийный сбыт по высоким ценам. Таким образом, информация, собранная исключительно в оперативных целях, позволила получить указания стратегического порядка.

Поэтому представляется рациональным объединение всех баз в рамках одной картотеки. Опыт показывает, что серьезная работа может начинаться со следующими базами: конкуренция (вся информация по действующим и потенциальным конкурентам):

- рынок (вся рыночная информация, вкусы и запросы потребителей, каналы сбыта и т.п.);

- технология (производства и использования продукции);

- законодательство (вся информация по законодательству, затрагивающему деятельность фирмы, а также информация по деятельности органов,

разрабатывающих и принимающих новые законодательные положения);

- ресурсы (вся информация по материально-техническим ресурсам, необходимым для нормальной деятельности фирмы, по сырью, поставкам, рабочей силе и финансам); общие тенденции (политическая, экономическая, социальная, демографическая и т.п. информация);

- прочие факторы, влияющие на деятельность предприятия (факторы, не учтенные в предыдущих базах).

Метод «ЗВ» позволяет вам обеспечить наблюдение за нужными вам базами. Однако ваше предприятие развивается, могут появиться новые цели, рынок и окружающая среда постоянно изменяются. Поэтому вы должны предусмотреть возможность периодического пересмотра ваших баз на основе повторного анализа целей и потребностей вашего предприятия.

Таким образом, даже ценная информация, которая зачастую добывается с большим трудом, должна вовремя поступить тому, кому она необходима. Информация является ценной только тогда, когда она может использоваться. Если информация не служит для принятия решения, то она является беспредметной, а, следовательно – несуществующей. Естественно, на основании этой информации может быть принято решение ничего не предпринимать, что такие является одним из типов принимаемых решений и способом использования информации. Одним словом, информация является незаменимым сырьем для выработки любого решения, таким же сырьем, как и любое другое, которое необходимо добыть, переработать и поставить до истечения срока годности тому, кому оно необходимо.

Упражнение. Составьте для вашего предприятия основные базы для наблюдения, руководствуясь в случае необходимости следующими факторами: конкуренция; рынки; технологии; законодательство; ресурсы; общие тенденции.

Ключевые положения. Для получения качественной информации необходимо: сформулировать цели, определить потребности, построить базы для наблюдения. Для деятельности предприятия, обычно, достаточно шесть баз для наблюдения: конкуренция; рынки; технологии; законодательство; ресурсы; общие тенденции.

3.2. Каналы информации

Канал текст. Подход к этим источникам в основном легок и дешев. Пусть информация не совсем точная, но она свежая. Например, за неделю до выпуска новой продукции появлялись сигналы в широкой прессе, за месяц – в специальной и за полгода – в банке данных. Свежесть информации – это очень важный критерий для выбора между двумя важными каналами: текст и фирма. Каждый из них представляет 30 – 40% полной информации, господство преимущества канала текст распространяется на промышленные предприятия, а фирмы – на коммерческие предприятия. В большинстве случаев они оба должны быть использованы как дополнительные. В настоящее время насчитываются десятки миллионов публикаций. Когда вы приступаете к обсуждению нового вопроса, начинайте с запроса периодики,

охватывающей данную область, если нет специального, посвященного данной теме издания. Часто это является наилучшим способом получения информации, имен экспертов и учреждений.

Канал фирма. В этот канал входит весь персонал предприятия, который может и должен вступать в контакт со сторонними организациями в связи с информацией: коммерческой, технической, финансовой, юридической и т.д. По своей природе он покрывает значительные неравные базы: 60% информации, проходящей через него, относится к группе «конкуренты–рынок–ресурсы», 15% – технологии, 15% – регламентирующие документы, 10% – тенденции развития. Именно поэтому необходимо относительное равновесие в самом канале.

Самую большую группу действующих кадров образуют клиенты, поставщики, агенты и распределители. Информация, а они ею владеют, циркулирует среди коллег или, по крайней мере, на собраниях и совещаниях. Необходимо сделать такую диффузию более эффективной, чтобы информация попадала по назначению в нужное время, необходима определенная организация информации с учетом гибкости, позволяющей ее беспрепятственное движение. Таким образом, наилучшее средство состоит в перегруппировке некоторых лиц в сети корреспондентов. Они должны в совершенстве разбираться в своей области для приема и интерпретации сигналов, даже самых слабых и гуманных, что позволит вступать в правильный контакт как вне, так и внутри фирмы и получить возможность и желание общаться.

Канал консультант. Этот канал в основном охватывает базы регламентирующих документов, источников и тенденций. С помощью знания этих трех составляющих, часто проходящих статистическую компиляцию, эксперты извлекают информацию, имея привилегированный доступ к определенным источникам. Эксперт не всегда является посторонним лицом для фирмы. Экспертная оценка может даваться компетентным лицом го числа сотрудников данной фирмы. Такие «фирменные эксперты» могут быть постоянными или временными. Последние разгруппированы и собираются каждый раз, когда появляется необходимость в информации, входящей в круг их компетенции. Постоянные эксперты, организованные в общества по исследовательской деятельности и обработке информации, делают заключение относительно сообщений, они редактируют итоги конференций и получают информацию по интересующему их вопросу.

Работа консультантов и обществ сторонних служб более деликатна, поскольку это посторонние органы, которые могут провоцировать на предприятии нарушение равновесия и отрицательные реакции. Вот почему их внедрение, сниженное до необходимости, должно всегда быть тщательно подготовлено.

Канал беседа. Через этот канал обычно проходит немного информации, но она должна обнаруживать большую точность. Нельзя в этом проявлять небрежность. Те, кто полагается на ее очевидность, должны быть очень хорошо подготовлены, особенно в знании того, что входит в круг интересов предприятия. Недостаточно одного брифинга для того, чтобы прийти к нужному выводу или контакту. Чтобы извлечь больше выгоды от ярмарок и салонов, приготовьтесь к визиту, предварительно прочитав каталоги. Если возможно, пойдите вдвоем, пока один представляет на стенде основные пустоты, другой в это время наполняет сумку документацией и делает при случае фотографии.

Научные и технические конференции – удобный случай для инженеров и

исследователей собраться и вдоволь наболтаться. Экспертная фирма, от которой требуется внимание к определенным вопросам, сможет дать точные определенияпо своему вопросу, побывав там.

Канал джокер. Иногда случается, что информация попадает в поле зрения совершенно неожиданно: поставщик забыл свой перечень поставок в ресторане или в самолете, перехватывается беседа, жена сообщает признания соседки о компании, где работает ее муж, встречаются на улице старинные приятели и т.д. Если эта информация не отбрасывается априори, всегда благоразумно не рассчитывать на случай, а лучше поработать, задействовав 4 основных канала.

Методика 4К+1. Для получения свежей информации нужно найти контакт с тем, кто находится вблизи событий. Эти эксперты в силу своего знания данной области, своих записных книжек, содержащих адреса и телефоны своих коллег по службе из различных лабораторий, своего участия в конференциях должны были бы знать заранее о том, что готовится некоторое действие со стороны конкурента.

Методика поиска информации, которая называется 4К+1 (1 – часть, соответствующая джокеру), имеет тотальную ценность. Она применяется, например, полицией для поиска преступников. Например, проследим приключения двух детективов, которые ищут преступника. Преступник становится продавцом. Капитан обращается к своим любимым детективам и поручает им это дело. И что же делают эти полицейские? Прежде всего, они погружаются в архивы, чтобы найти аналогичные дела и отобрать имена некоторых подозреваемых. На этом этапе они используют канал текст. Затем они обращаются к своим коллегам, так называемой внутренней сети, чтобы лучше разобраться. Они расспрашивают полицейских, которые ранее арестовывали этих подозреваемых, о психологическом типе преступников; принимают решение провести расследование вблизи патрулирующих служб и т.д. Наконец, они находят осведомителя, который играет роль «консультанта». В центре своего нового ресторана он им сообщает о слухах. Посредством этих трех каналов наши детективы экономили много времени при получении необходимых им сведений для ареста преступника. Канал беседа используется крайне редко. Он соответствует, например, Интерполу при встречах с различными полицейскими службами. Джокер служит больше всего в сериалах, к нашему превеликому удовольствию, чем в реальности (прядильные фабрики, ночные визиты подозреваемых, взломы сейфов, внезапно взявшиеся ниоткуда свидетели).

Поиск источников. Теперь бы располагаете всем набором средств, позволяющим вам разрешить любую проблему поиска информации. Кратко обобщим:

1. Методика 4К-1 в форме «моросящий дождь». Формальное функционирование службы информации достаточно однообразно. Базы наблюдения подписываются регулярно четырьмя каналами. Отсюда и скучное название «моросящий дождь». Для того чтобы дать своевременный ответ или обнаружить опасность путем наблюдений по каналу джокер, необходимо постоянное пополнение информации. Такой образ функционирования системы называется «гроза», т.к. он позволяет быстро получить большой объем справочной информации. Следующие четыре методики относятся к этому типу функционирования системы.

2. 4К+1 по методу «гроза». Прежде, чем заниматься поиском информации в неподходящих местах, следует удостовериться, что она еще не получена. Нужно

начинать свои действия, активизируя разнообразные каналы, особенно два основных: Текст и Фирму. Вы просите, например, ваших внутренних корреспондентов собрать всю необходимую вам информацию.

3. Семейства источников. Если предыдущие поиски долго не завершаются или вы пришли к выводу, что немного шансов быстро завершить поиск в силу экстраординарности проблемы, обращайтесь к источникам. Чтобы это сделать, вам необходимо установить интересующие вас семейства источников, проделав предварительную работу с самим источником, чтобы выяснить, содержит ли он поисковую информацию (или насколько велики шансы ее содержания в нем). Все это необходимо для того, чтобы определиться в форме представления и доступа к информации. Вы сможете, наконец, подойти вплотную к стратегии захвата источника. Такая методика, как и последующие, намного сложнее и дороже, чем предыдущая. Итак, дважды удостоверьтесь, не получена ли справочная информация по традиционным каналам. Часто случается, что руководители теряют дни и недели, предпринимая сложные маневры для получения информации, которая находится в простом отчете служебной документации.

4. Тропинка информации. Если проблема по своей природе не может быть отмечена среди семейств (потенциального источника), тогда вам необходимо восстановить тропинку продвижения информации для определения различных сделок и восстановления хода события. Предположим, что вы бы хотели определить место расположения нового завода одного из ваших конкурентов. Обычная покупка территории приводит в действие целый каскад событий и вовлекает большое количество действующих лиц: должностные лица, юристы и финансисты предприятий, продавец, агенты по недвижимости, нотариус, страховые службы, банки и т.д. Столько же потенциальных источников. Остается определить какой из них подходит и доступен. Иногда информация имеется в распоряжении экспертов, публикаций, банков данных, библиотеках, т.е. стандартных источников. Иногда информации просто нет. Например, количество существующих или готовящихся к открытию обувных магазинов, расположенных в определенном районе. Как же в таком случае получить информацию? Перелистать ежегодник «желтые страницы», просматривая рубрику «обувь» и отмечая адреса магазинов, расположенных в интересующем квартале. Итак, источник восстановлен. Источник может быть всегда восстановлен, если существует информация, но не всегда оказывается доступным, если не учитывать способов, которые не входят в компетенцию предприятия. Классический пример. Как установить эксплуатационную способность нефтяной компании? Многое указывает на то, что это зависит от глубины скважин, а это как раз относится к тем сведениям, которые компания совершенно не собирается предоставлять. Существует довольно простой способ это определить: он состоит в том, что нужно запастись биноклем и подсчитать количество труб, подвозимых к местам бурения. Нужно умножить количество труб на их длину, чтобы определить глубину скважины. Этот последний пример показывает важность наблюдения для получения непосредственной информации. Если, например, вы интересуетесь рынком микроинформатики, вы замечаете, что количество произведенных клавиатур совладает с количеством произведенных экранов. Создаваемая клавиатура явится основным индикатором для воссоздания источника.

Таким образом, если вы захотите узнать количество микроЭВМ, выпущенных какой-то компанией, вам нужно выяснить, сколько клавиатур» она закупила. Чуть ли не все турбины в мире используют патент Дженерал Электрик. Заявка на лицензию –

хороший индикатор определения проекта нового электродвигателя.

5. «ЗВ». Если судно плывет в полном тумане или точка отправления настолько туманна, что продвижение само по себе оказывается невозможным, шанс есть и не остается ничего иного, как использовать единственный способ: применить метод «ЗВ», полностью подходящий для решения такой проблемы. Например: Цель. Узнать результат деятельности завода, который не публикует ежегодных отчетов, т.к. считается ядром большой группы, занимающейся разнообразной деятельностью. Необходимость. Поскольку не ставится задача получения сведений нелегальным путем, нужно постараться выстроить свои расчеты, оценив поступление и выход денег. Базы. Входы – продажа; выходы – зарплата персонала, сырье, разнообразные ресурсы (вода, электричество и т.д.).

Источники. Для каждого входа и выхода необходимо сконцентрировать усилия на определении одного стандартного или нестандартного источника. Если не предполагается сезонная деятельность, решение состоит в том, что нужно расположиться на несколько дней перед входом на завод и подсчитать: количество выезжающих грузовиков с конечным продуктом; количество и вид грузовых автомобилей поставщиков; количество людей, идущих на работу. Зная природу транспортируемой продукции, возможно оценить стоимость каждого груза. И зная природу деятельности, можно оценить различных потребителей. Наконец, войдя в контакт с несколькими рабочими в баре, можно получить по одному лишь внешнему виду представление о средней заработной плате. И остается лишь проделать некоторые арифметические действия для воссоздания расчетов по данному заводу. Это кажется громоздким, но часто полезно для приблизительного подхода. В противном случае возможны уточнения.

Упражнение. Выберите тему, по которой вы бы хотели получить информацию (идентификация военного самолета, определение ведущей страны, знание основных цен рынка на определенные поставки и т.д.) и примените последовательно 5 методов исследования: 4К-1 в форме «моросящий дождь»; 4К+1 по методу «гроза»; семейство источников; тропинки информации; «ЗВ».

Полезная информация не является секретной. Адмирал Захария, шеф разведслужбы американского флота во время второй мировой войны, имел обыкновение говорить: «Большая часть полезной информации – 95 % не является секретом». Эти 95 % так называемой открытой информации, более или менее доступной, не составляют тайны. Но, если возможно одним телефонным звонком узнать курс марганца в Лондоне, то невозможно получить список членов Клуба конного спорта таким же образом. Хотя он и не является секретным. Это обращает внимание на то, что следует различать открытую информацию от информации, являющейся достоянием общественности, к которой доступ имеют все, а также информацию частную, которая и является объектом поисков условий допуска к ней.

Информацию, являющуюся достоянием общественности, не следует считать опубликованной! Например, закон дает своим гражданам право доступа к различным административным досье (здравоохранение, налоги, судимости и др.), но запрещает их публикацию.

Информация частная, как и частная жизнь, не является секретом, но подпадает под контроль тех, кого она касается. Например, список банковских клиентов и счетов,

перечни частных клубов и т.д. Что же такое секрет и чему он служит? Секретом можно назвать то, что держится в стороне, вдали от посторонних глаз. Речь идет о такой информации, которая по политическим или коммерческим соображениям считается ключевым моментом определенной ситуации. Такой случай – «секрет атомной бомбы» в проекте Манхэттена, шелка в Китае, в наше время – Кока-кола. Секреты промышленные в основном относятся к производству, зависящему больше от искусства, чем технологии, что дает решающее преимущество перед конкуренцией. Они должны быть охраняемы, откуда иногда смешение понятий зашита информации и сохранение секретности.

Упражнение. Вы владеете формулой Кока-колы. Подскажите сценарий, который, оставаясь в рамках закона, позволил бы вам проделать некоторые действия. Напомним, что само по себе владение секретом не является доказательством его подлинности. Напомним также историю одного бестактного служащего крупного предприятия, который собрался предложить несколько «горячих» документов конкуренту и был арестован полицией, поднятой по тревоге последним.

Ключевые положения. 95% информации не является секретной. Информация открыта, если она доступна всем, представляет частный интерес, если ее распространение ограничено определенными условиями. Пять методов поиска информации:

- 4K+1 по типу «моросящего дождя»: предприятие постоянно получает соответствующую информацию в базы по каналам Текст, Фирма, Консультант, Беседа и Джокер.

- 4K+1 по типу «грозы». Предприятие мобилизует свои каналы в случае настоятельной необходимости получения информации.

- Семейства источников. При непосредственном контакте насчитывается около 10 семейств источников (клиенты, поставщики, банкиры, службы компаний, распределители и агенты, консультанты и эксперты, широкая пресса, специальная пресса и банки данных, администрация, ярмарки и конференции).

- Тропинки информации. Позволяют определить сделки и соглашения для того, чтобы непосредственно возвратиться к самому событию.

- Методика «3В» применяется в особых случаях, когда все остальные потерпели неудачу или оказались мало полезными.

3.3. Обработка информации

Химики изобретают новую молекулу, инженеры находят средства ее производить, рабочие обеспечивают надлежащие условия производства, фармацевты ее распределяют... и теперь она кажется исчезнувшей в воде. Впрочем, то же самое, что происходит с информацией: ломают себе голову, чтобы уточнить необходимости, знают, что нужно наблюдать, находят источники, все знают заранее, что готовится нечто важное и когда событие происходит, не остается от работы ничего, кроме пузырька воздуха. В действительности информация – такая же продукция, как и прочие и процессы поиска, обработки сравнимы с промышленными или скорее с

добычей железной руды.

Первый этап (ЗВ) гарантирует только обзорную информацию, так называемую адекватность потребностям организации. В конце концов, ее необходимо проанализировать, чтобы удостовериться в надежности информации, сделать синтез для получения полного образа, начиная с разрозненных остатков до полной уверенности во всеобъемлемости. Таков полный цикл информации.

Обработка информации. Представим, что конкурент сообщает о внезапном увеличении мощности выпуска продукции. Прежде, чем это исследовать, необходимо узнать точную ценность этой информации. Возможно, она правдива, и в этом случае требуется
определенная линия поведения. Может быть она ложна, тогда это несколько иначе характеризует конкурента и требуется совершенно отличная от прежней линия поведения.

Без хорошей оценки есть риск принять пузыри за фонари и оказаться, в конечном счете, газовой горелкой в воде. Иначе говоря, необходимы разнообразные операции между получением и распределением информации с целью гарантировать пользователям безупречную продукцию: они должны получить все, что им необходимо и все, что они получают, должно быть незамедлительно использовано. Первой и самой важной операцией является анализ, который служит дополнительным фильтром, отбрасывающим ненужное и являющимся зашитой от шума без основания. Эта операция состоит, прежде всего, в определении важности, точности и значимости информации.

Важность информации. Построение баз наблюдения согласно с процедурой ЗВ гарантирует связь с наблюдаемой информацией. Но информация, связанная тематически, может не иметь особого значения. Для производителя автомобильных деталей информация, согласно которой Рено собирается закрыть завод в Вийанкур, связанная, поскольку все, что касается автомобилей, имеет к нему отношение. Но она не важная, т.к. глобальная мощность Рено не меняется, это решение не производит на изготовителя запасных частей особого впечатления. И, наоборот, для этого же производителя сообщение о компании Рено-Вольво может оказаться очень важным, если предполагается проведение некой стандартизации. Информация является важной, если она связана, т.е. имеет связь с элементами базы, и если она способна внести вклад в организацию. Когда вклад значителен и непосредственен, информация требует срочных действий. Информация, не имеющая значения, должна быть исключена во избежание потери времени и энергии.

Точность информации. Не всегда легко установить, является информация достоверной или ложной, особенно, если она содержит сведения о событиях, которые еще не произошли. Допускается два критерия, по которым можно судить о точности информации: надежность источника и самой информации.

Главным критерием правдоподобия является поиск подтверждения по другим источникам, если возможно, независимым. В случае получения информации от стороннего наблюдателя, клиента или поставщика, о том, что конкурент готовится наладить выпуск новой продукции, можно считать ее достоверность установленной. К сожалению, обычно располагают лишь одним источником, когда речь идет об очень светских новостях. Решение состоит в поиске связанных событий в различных

сообщениях. Вы узнаете, например, в вашем рекламном агентстве, что конкурент, возможно, собирается сменить агентство. Короткий шум, в другом месте, а ведь это он готовит выпуск новой продукции. Две информации стыкуются. За неимением таких связок вы должны полагаться на свой опыт или на опыт экспертов, чтобы составить правильное суждение об информации. Судить о кредите по одному источнику не проще. Только опыт позволяет быть уверенным: чем дольше источник поставлял ценные сведения, тем менее весомы основания для сомнений в точности сведений. Если такового опыта нет или источник новый, вы должны, прежде всего, задаться вопросом, позволяет ли положение лица, передающего сведения, иметь доступ к сообщаемым фактам. Наконец, вы должны задаться вопросом мотивации. Кандидата на работу, который вдруг спонтанно дает информацию о своем предыдущем работодателе, не следует подозревать в лукавстве: он пытается хорошо выглядеть для получения должности. Напротив, подозревайте того, кто дает информацию без всяких видимых причин. Наконец, продумывайте условия, при которых информация была вам преподнесена. Трудно, например, доверять признанию, сделанному в баре между двумя рюмками виски в три часа утра.

При отсутствии надежности источника или информации, не следует ее отбрасывать, особенно, если она производит впечатление важной. Вы должны просто отложить ее про запас в ожидании новых элементов, позволяющих вам подтвердить ее или отвергнуть.

Значимость информации. Информация может быть важной и точной и в то же время бесполезной, поскольку она недостаточна для понимания и действия. То, что конкурент меняет рекламное агентство – информация важная, но в изолированном виде она сообщает немного. Ее следует не отбрасывать, а соотнести с другой информацией, что может принести явную пользу.

Два понятия, проведенные раздельно или параллельно, позволяют судить о значимости информации. Первое называется «циркуляция». Оно состоит в быстрой циркуляции информации среди лиц, имеющих к ней отношение, в надежде на возможность установления связи с иной информацией. Ваш коммерческий директор определенно установит связь между изменением рекламного агентства и слухом о готовящемся выпуске новой продукции.

Второе понятие называется «синтез». Оно состоит в соединении всех обрывков информации, что похоже на сбор головоломки, для воссоздания полного образа. Это не всегда легко, потому, что часто не достает частей или они неподходящей формы. Иногда наоборот, части идеально подходят, давая ясное представление о ситуации: закрытие завода, изменение линии продукции и анализ баланса позволили предприятию понять, что у конкурента были трудности с государственной казной. Чаще приходится проделывать определенный путь при формировании гипотезы: попытку синтеза, циркуляцию, связав это с исследованием вспомогательной информации для того, чтобы добиться ясного и полного образа. Эта формулировка подходит для самых тонких гипотез. Причиной многих катастроф является не пренебрежение информацией, а ошибочное ее понимание. История насыщена множеством примеров, особенно военных, где последствия серьезны и наглядны. Израильская разведка, которую часто совершенно справедливо и заслуженно превозносят, тоже допустила несколько промахов: не предвидела ни войны Иома Кипура в октябре 1873 г., ни резкого поворота Садата в 1977 г., ни Интифада 1987 г.

Но, что касается поставки точной информации, относительно тактических операций, израильская разведка не имеет себе равных. Напомним разрушение центрального иракского ядра в 1981 г., шестидневную войну (1967 г.) или налет на Ажио (1978 г.). И наоборот, когда требуется опередить стратегические движения противника, она так же неповоротлива, как и другие, потому что пренебрегают широким обзором и методикой.

Как же следует действовать, чтобы восстановить гипотезы и также придать смысл фактам, на первый взгляд кажущимся смешанными? Прежде всего, нужно уметь пренебрегать предубеждениями. Если недооценивается противник, он будет пытаться исключить априори определенные гипотезы, и 9 к 10, что он поймается: американцы недооценили дух независимости вьетнамцев, израильтяне недооценили способность палестинцев к бунту на оккупированных территориях, западные предприниматели недооценили японское наступление в 70-е годы. Если легко выразить принцип пренебрежения своими предубеждениями, то трудно его применить, поскольку не часто совершаются одни и те же ошибки. Главное и несомненно единственное решение: чтобы избежать ловушки, необходимо запросить мнение совершенно различных лиц, насколько это возможно. Это позволит не только сличить мнения, но и получить сведения по определенным предположениям и даже больше.

Два вспомогательных подхода позволяют получить свидетельство набора информации. Первый называется «расширение» и второй называется «намерение».

Подход по методу расширения состоит в том, что для данных, имеющихся в распоряжении, подыскивается наиболее соответствующее объяснение. Часто при завершении различных гипотез обнаруживаются противоречия. Например, фотографии со спутников указывают, что войска противника пришли в движение, и взрыв транспорта с радиоактивным топливом разоблачает крупное перемещение в стане противника. Эти два факта могут сигнализировать о больших маневрах, либо о подготовке к войне. В такой ситуации благоразумно придерживаться худшей гипотезы. Важно найти всю информацию, способную подтвердить такую гипотезу (имеется в виду война) и отбросить другую, но не наоборот.

Подход «намерение» состоит в обнаружении того действующего лица, в намерения которого входят последние факты, Внимание! Не начинайте думать за кого-то. Просто поставьте себя на его место, чтобы понять, какую игру он ведет, чтобы сделать вывод о его возможных действиях. Исходя из этого, строится множество гипотез относительно его намерений и исследуется, как они должны были бы объяснить факты. Наконец, сравнив предполагаемые факты с имеющимися в наличии данными, выбирается гипотеза (или гипотезы), которая охватывает самый большой диапазон наблюдений.

Представьте, например: Япония, небольшой остров (примерно половина Франции), сильно индустриализована, но практически лишена каких бы то ни было запасов сырья и от того не очень любит еще с войны всю Азию, особенно своих самых близких соседей – корейцев и китайцев. При таких условиях один из самых решающих вопросов, который задается японцам – это снабжение продовольствием. Рассматривая карту, вы обнаруживаете, что Сибирь со своими огромными ресурсами находится относительно недалеко и имеет прямой доступ. Вы, впрочем, знаете, что для улучшения этого сурового края Советы пренебрегают капиталом и технологией, а именно этого японцам не занимать. Вы скажете, что такое сопоставление Японии и Советского Союза требует пристального рассмотрения. К сожалению, отношения

между двумя державами уже давно натянуты из-за Курильских островов (архипелага, который Советы отняли у Японии). И вот в марте 1990 г. член японского парламента предложил откупить два острова. Эта идея кажется нелепой, но соберитесь с мыслями, когда вы принимаетесь за рассмотрение точки зрения японцев и Советов. Это именно тот случай, когда вы можете пробовать истинно проникать в мышление другого и получать в итоге четкий свой проект.

Анализ, синтез, циркуляция составляют основные операции обработки информации. Конечно, можно рафинировать, снимать кожуру в соответствии с гораздо большим количеством критериев, или пробовать организовывать информацию в соответствии с более сложными образами. Но опыт лишний раз доказывает, что лучшее – враг хорошего.

Циклы информации. Руководитель, который впервые принимается за исследование информации, охотно верит, что он натолкнется на скудность источников. Применив методику – 1К-1, он вскоре поймет, что оказался перед изобилием источников. Отсюда неизбежен вопрос: так ли необходимо подписываться на 500 газет, подключаться к 50 банкам данных и говорить с 300 собеседниками? Иначе говоря, как убедиться, что источники полезны и немногословны? Единственное средство – постоянная проверка источников по двум простым критериям: обеспечение и эффективность.

Обеспечение источников. Подписываются ли все базы информацией? Если ответ негативный, этот источник определенно не подходит. Его следует заменить. Все ли источники снабжаются полезной информацией, т.е. важной и точной? Ваша служба, ведущая документацию, должна исключить целый ряд дорогостоящих публикаций, не представляющих интереса. Поставляют ли определенные источники систематизированную информацию? Как часто цитируется информация? Необходимо исключить многословие. Эффективность источников.

Информация называется свежей, если интервал между самим событием и сообщением в нем короткий. Если, например, вы узнаете, что бессонные ночи главного руководства конкурентного предприятия проистекают от решения по внедрению новой продукции за шесть месяцев до ее выпуска, вы располагаете информацией большой свежести, которая оставляет вам время отреагировать. Если, наоборот, вы узнаете об этом только в день официального сообщения, то эта новость немного запоздала и тут уже мало, что можно сделать.

Свежесть и конфиденциальность – два качества, дополняющие одно другое, помогают судить о полезности источника. Если вы констатировали, что в своей области вы располагаете только конфиденциальной информацией, не охваченной широкой прессой, у вас появляется интерес обратиться к экспертам, имеющим более близкое отношение к явлению. Поскольку каждое действие изменяют предприятие, его люди постоянно перемещаются, иногда необходимо проверять базы, обуславливающие весь путь получения информации, а также соответствие источников целям и необходимостям. Два типа событий могут привести к модификации. Первое относится к резкому изменению жизни предприятия, такому, как появление нового рынка, революционной технологии, смена руководства и т.д. В таком случае достаточно применить путь 3В.

Труднее обойти случай медленного развития, который дает меньше неадекватных баз. Вы это замечаете, когда пользователи информации все более и более недовольны,

обнаруживая, что они получают мало полезного для принятия своих решений. Единственным средством ухода от этой проблемы является организация регулярных встреч поставщиков информации с пользователями. Система, пожалуй, пребывает более 99% времени, она функционирует некоторым образом сама по себе без излишней необходимости в постановке вопросов. Имеется определенное количество источников, которые снабжают информацией, собираемой по схеме ЗВ и выверяемой путем отбора источников. Как известно, развитие – это очень быстрая операция; и накопление, и распределение происходят в суматохе. Напомним, что сам по себе сбор информации не представляет трудности, поскольку он имеет хорошую «картографию» окружающей среды. Остается менее 1 % времени, когда нужно больше работать головой. Первое размышление должно привести к источникам, проверке их охвата базы и эффективности: это малый цикл информации. Второе размышление должно подвести к самим базам для выявления того, какие из них соответствуют на сегодняшний день целям и потребностям организации: это большой цикл информации.

Особо ценная информация. Эффективность службы информации не только сводится к сбору фактов и их передаче. Информация существует как связь с намерением. Если нет «направленного движения», усилия «прямо к цели», то и необходимость в такой информации равна нулю. Чтобы лучше рассмотреть проблему дополнительной ценности, полезно разделить решения на два типа: те, для которых информация первична и те, для которых первична проблема. Информация первична, когда решение прямо вытекает, т.е. без тех или иных фактов решение не существует.

Поскольку информация первична, ее ценность очевидна. Проблема первична, если информация должна подтвердить решение. Это получение справок по политике и экономике различных стран путем консультаций у нескольких экспертов по вопросам технологии. Вот такую дополнительную ценность, полученную из изолированной информации, гораздо труднее оценить. Дополнительная ценность приобретается в тот момент, когда информация влияет на принятие решения. Информация – это продукция, она проходит длинный цикл – приобретение, обработка – распределение – каждый имеет стоимость и цену. К сожалению, стоимость и ценность не всегда может быть выражена в цифровом отношении: за информацию часто платят информацией и она соединяется в единое неделимое целое. Вот почему службу информации не следует рассматривать как центр доходов.

В заключение, информация предлагает дополнительную ценность, когда она прямым или косвенным образом принимает участие в решении. Бездействие – это тоже форма действия, даже когда обдумывается выбор. Не ожидайте, что каждая информация приведет к большим результатам.

Создавать ценную информацию – прежде всего дело организации. Снизу вверх, организация пространства действий благодаря ЗВ для сбора необходимой информации и никакой иной. В центре, организация самой информации для прояснения ситуаций априори сложных и смешанных, подвергающаяся такой обработке, что весь персонал, имеющий к этому отношение, получает вовремя необходимую информацию. И параллельно, сама организация деятельности такова, что каждый чувствует себя причастным к жизни предприятия: «Информация – кровь предприятия», гласит девиз Мицуи, который преуспел. Только при таких условиях предприятие существует и развивается, получая необходимую суть своего ново

обращения, избегая информации сложной или ее утечки.

Ключевые положения. Обработка информации:

- анализ информации: важность, точность, значительность;

- синтез: подход путем расширения, подход путем намерения

- развитие источников: обеспеченные, эффективные.

Система стратегической информации. По каналам «Текст» и «Фирма» поступает 80% информации, необходимой предприятию. Поэтому Система стратегической информации (ССИ) должна строиться вокруг этих двух каналов. Большие различия природы и механизмов функционирования этих каналов вынуждают разделять две области деятельности:

1. Система стратегической и перспективной информации (ССПИ) обслуживает каналы «Текст» и «Консультант», т.е. занимается текстовой информацией, а также информацией, поступающей от экспертов, консультантов и фирм, оказывающих консультационные услуги. Эта система выполняет, главным образом, стратегическую роль, а ее деятельность ориентирована на перспективу. Персонал этой системы имеет университетскую подготовку или подготовку журналиста, специализирующегося в области экономики или политики.

2. Система тактической и оперативной информации (СТОИ) обслуживает каналы «Фирма» и «Беседа». Она использует контакты сотрудников фирмы с внешним миром, а также все возможности меж профессиональных встреч, таких как ярмарки, выставки и конференции (только узкоспециализированные, например, научные конференции). Персонал этой системы должен обладать отличным знанием ситуации на местах, различных специальностей и профессий, а также деятельности фирмы. Минимальным предварительным требованием является более чем 5-летний опыт работы на ответственных оперативных постах и, по возможности, в различных странах. Гармонизация функционирования этих двух систем является сложным делом. Если ССПИ доминирует над СТОИ, то информация может оказаться по своей природе непригодной для руководящих работников и специалистов, занимающихся оперативными вопросами. Если же доминирующую роль играет СТОИ, то информация ограничится сферой профессиональных интересов работников, которые занимаются ее сбором, а целостные базы данных будут игнорироваться.

Существует два способа координации деятельности ССПИ и СТОЙ: один – в рамках централизованной организационной структуры, другой – в рамках децентрализованной.

Централизованная организационная структура. ССПИ подчинена непосредственно генеральной дирекции. В ССПИ в централизованном порядке поступают все данные, собранные СТОИ каждого департамента или подразделения. Преимущества централизованной организационной структуры заключаются в возможности координации тех усилий, получения экономии за счет эффекта масштаба, получения целостной общей картины происходящего, а также сопоставления самых различных данных с целью получения стратегической информации. Однако такая

организационная структура является малоэффективной в условиях многоотраслевой фирмы, когда множественность разнообразных информационных потребностей превышает возможности обработки информации и компетентности работников.

Конечный информационный продукт, полученный в результате обработки информации и различных соображений, поступающих из разных департаментов и подразделений, может вполне уподобиться некоторым резолюциям парламентских комиссий, которые стремятся предусмотреть все возможные случаи, никого при этом, не обидев, а потому не представляют ни малейшего интереса.

Опорой централизованной системы нередко являются один человек или группа работников, которые рассматривают успех ССПИ в качестве своего личного успеха. Если такая система теряет своего лидера или кого-либо из лучших работников или даже своего главного покровителя в генеральной дирекции, то она может попросту развалиться. Централизованная система стратегической информации. Для того чтобы централизованная система работала эффективно, а департаменты и подразделения делились информацией, крайне необходимо, чтобы ССПИ не воспринималась в качестве «игрушки» одного человека.

Децентрализованная организационная структура. Каждый департамент или подразделение располагает своей собственной системой стратегической информации (ССИ), которая сочетает функции ССПИ и СТОИ. Информационные сводки, подготовленных этими службами, поступают в ССПИ, подчиненную генеральной дирекции.

Преимущество децентрализации заключается в полном соответствии непосредственным текущим потребностям отдельного департамента. Кроме того, каждый занимается только тем, что имеет к нему прямое отношение, что значительно упрощает управление информационными потоками.

Однако децентрализованная система имеет свои недостатки. Так как каждый департамент или подразделение занимается сбором и комплексной переработкой (обработка, хранение, распространение) информации по полному циклу, то проблема персонала крайне усложняется: средств и возможностей одного департамента или подразделения может оказаться недостаточно для найма или привлечения необходимых специалистов. Если же поручить эту задачу кому-либо из уже имеющихся работников в качестве дополнительной работы, то это может закончиться тем, что ничего не будет делаться.

Кроме того, отдельные департаменты или подразделения могут иметь стратегические цели и интересы, отличные от целей концерна, что до предела осложняет работу ССПИ, подчиненной генеральной дирекции.

В тех случаях, когда различные департаменты и подразделения действуют на одинаковых или сходных рынках, а также когда они конкурируют с одними и теми же фирмами, нередко имеет место ненужное дублирование усилий. Кроме потерь времени и денег, такая конкуренция между департаментами или подразделениями может полностью заблокировать обмен информацией.

Децентрализованная система стратегической информации. Таким образом, идеальной универсальной системы организации не существует. Однако возможен любой промежуточный вариант между централизованной и децентрализованной

системами. В конечном счете, это зависит от типа предприятия и характера его деятельности, то есть от таких параметров:

- узкоотраслевой или многоотраслевой характер деятель ноет фирмы, ориентация на один или несколько рынков;

- централизованная или децентрализованная система управления предприятием и, в частности, система стратегического планирования:

- наличие или отсутствие системы обмена информацией между департаментами или подразделениями.

Главное заключается в обеспечении максимально быстрого обмена и прохождения информации, независимо от принятого типа организации ССИ. На уровне СТОИ это означает, помимо всего прочего, что следует опасаться излишнего формализма. Разумеется, для обеспечения внутренних связей и стройности системы определенный минимум формализма необходим, но при этом следует избегать бесполезного бумаготворчества и прочих административных излишеств, которые могут вызвать неприятие со стороны сотрудников фирмы, работающих на местах.

На уровне ССПИ следует всячески поддерживать и развивать контакты между департаментами или подразделениями фирмы. В конечном счете, речь идет, прежде всего, о человеческих отношениях и мотивации работников.

Внедрение системы стратегической информации. Предприятие, принявшее решение о создании системы стратегической информации (ССИ), нуждается в информации для обеспечения своей деятельности. Поэтому создание ССИ должно начинаться с уточнения его целей, а также наличных и недостающих средств. Для этого необходимы:

- создание комитета стратегической информации;

- назначение будущего руководителя ССИ;

- анализ информационных потоков.

Комитет (ССИ) объединяет основных потребителей информации, т.е. руководящих работников высшего ранга и специалистов из дирекции, с целью определения профиля и задач ССИ.

Главная задача комитета заключается в подборе руководителя ССИ. Последний должен одновременно обладать высокой технической компетентностью и большими психологическими способностями. Это связано с тем, что одним из основополагающих элементов ССИ является внутренняя сеть. И если у руководителя ССИ не установятся хорошие взаимоотношения со всем предприятием в целом, то прохождение информации и информационный обмен могут оказаться заблокированными. Поэтому руководителя ССИ лучше всего подобрать из числа опытных и испытанных специалистов фирмы, а не приглашать со стороны. Кроме того, у руководителя ССИ должно быть полное взаимопонимание с президентом фирмы. Они должны действовать в тесном содружестве и согласии друг с другом, как капитан и штурман на морском судне. Капитан должен полностью доверять своему штурману, который заменяет ему глаза и уши, полностью при этом сохраняя свободу своих суждений. Штурман, со своей стороны, должен чувствовать и понимать потребности и

устремления капитана, даже если они остаются невысказанными. Он не должен бояться высказывать свое мнение, даже если оно может не понравиться капитану. У него должно быть достаточно смелости для того, чтобы прервать капитана и настойчиво попросить себя выслушать.

Руководитель ССИ занимается всей практической работой по созданию этой службы, а комитет выполняет в дальнейшем только консультативные функции. Руководитель ССИ подбирает персонал, строит базы данных, выбирает оптимальную систему организации за счет сочетания централизованного и децентрализованного принципов, распределяет задачи и функции между ССПИ и СТОИ, организует внутреннюю сеть, подбирает начальный массив источников текстовой информации, организовывает работу с документацией и хранение информации, разрабатывает процедуры связи. Но прежде всего, он проводит анализ информационных потоков.

Очень важно, чтобы этот анализ проводился кем-либо из сотрудников фирмы, так как это гаратирует уважительное отношение и соблюдение культуры отношений, принятых в фирме, и способствует преодолению организационных и человеческих помех и препятствий. Однако не следует при этом пренебрегать помощью консультанта, так как свежий взгляд со стороны позволяет выявить еще неиспользуемые залежи информации.

Информационный анализ преследует две цели: изучение потребностей и запросов потребителей, а также механизма функционирования информационных каналов. В качестве иллюстрации приведем несколько примеров анкет.

3.4. Планирование работы

План – это схематически записанная совокупность коротко сформулированных мыслей-заголовков, это «скелет произведения» (И.Н. Кузнецов, 2001). Примером плана к книге, правда очень общего, отмечающего лишь узловые разделы, является обычное оглавление. Проглядывая его, не читая самой книги, можно получить представление о ее содержании и схеме построения. План как форма записи обычно значительно более подробно передает содержание частей текста, чем оглавление книги. Форма записи в виде плана чрезвычайно важна для организации умственного труда, для развития навыка четкого формулирования и умения вести другие виды записей. По форме членения и записывания планы могут быть подразделены на простые и сложные. Сложный план в отличие от простого имеет ко всем основным пунктам еще и подпункты, которые детализируют или разъясняют содержание основных. План может быть записан в виде схемы, отражающей взаимосвязь положений. Это план–схема.

Достоинства плана. Удачно составленный план прочитанной книги говорит в конечном итоге об умении анализировать текст, о степени усвоения его содержания. План имеет ряд достоинств, которые выдвигают его, наряду с конспектами и тезисами, во вполне независимую, самостоятельную форму записи.

Самая короткая запись. Именно благодаря этому план легко совершенствовать как по существу, так и по форме, при этом вновь и вновь продумывая содержание предмета.

Нагляден и обозрим. Никакие другие формы записи, кроме плана, не могут в такой яркой и легко обозримой форме отразить последовательность изложения материала.

Обобщает содержание. Хорошо составленный план раскрывает и само содержание произведения. В этой записи есть уже элементы обобщения, которые могут быть далее развиты в тезисах, конспектах, рефератах.

Восстанавливает в памяти прочитанное. План помогает легче уяснить содержание, способствует ускоренной проработке материала. План, составляемый к крупным произведениям, которые прорабатывают продолжительное время, позволяет рационально, без большой потери времени перед возобновлением работы воспроизвести в памяти прочитанное ранее. При этом напоминает лишь самое главное, существенное, если, конечно, читатель хорошо овладел материалом.

Помогает составлению записей. Руководствуясь пунктами плана и обратившись к подлиннику, можно составить и другие, уже более подробные и обстоятельные записи – конспекты, тезисы, рефераты. С помощью плана составлять их проще. Даже если с момента составления плана прошло довольно много времени, он поможет созданию конспекта или тезисов.

Путем составления, например, подробного плана к конспекту можно легко и быстро выявить повторения и непоследовательность в изложении текста, улучшить запись, сделав ее логически четкой и последовательной. С помощью плана читатель сам контролирует степень усвоения текста (при самоконтроле подробные ответы на вопросы плана говорят о хорошем усвоении).

План настолько помогает сосредоточиваться даже при сильно рассеянном внимании и умственном утомлении, что его можно рекомендовать как стимулирующий внимание фактор. В этом случае обычно нет надобности составлять план ко всему материалу подряд. Достаточно сделать подробный план к двум-трем страницам текста, как работа, которая ранее не ладилась и шла вяло, начинает продвигаться быстро.

Попутное с чтением составление плана не позволяет отвлекаться, заставляет вникать в работу, в смысл читаемого, отображать его в виде заголовков содержания, мобилизовать внимание. А если читающий все же отвлекся, ему следует бегло прочитать пункты составленного ранее плана и мысленно раскрыть их содержание. Потерянная было связь, быстро восстановится. А при новом сплошном, дословном чтении книжного текста не только теряется время, но и повышается утомляемость. Вдумчивое чтение всегда сопровождается составлением – в уме или на бумаге – плана, отражающего содержание, его логику и последовательность. Отсюда вывод: чем лучше читатель озаглавливает содержание, тем продуктивнее он читает, облегчая себе при этом анализ и запоминание текста.

Все книги и статьи, конечно же, пишутся по плану, ему подчиняется содержание, но плана в виде частых подзаголовков или подробного оглавления в книге опубликовано может и не быть. Тем более его не дают к статьям. В этой традиции есть свой смысл. Читатель должен как бы восстанавливать план, то есть сам докапываться до смысла. При составлении плана во время чтения одновременно происходит выборка нужного, закрепление его в памяти, а в результате возникает понимание идей и последовательности их подачи.

Начало работы. План помогает активно читать источник, и нет смысла откладывать

его составление до повторного чтения, как иногда советуют. Это ухудшило бы первоначальное восприятие материала и необоснованно отодвинуло бы во времени составление записи. Поэтому, в отличие от конспектов и тезисов, которые действительно есть смысл делать только после полного прочтения материала и хорошего с ним ознакомления, пункты плана можно и нужно фиксировать немедленно, уже в процессе первоначального чтения, под первым впечатлением. Потом, в дальнейшей работе, план может исправляться и уточняться. Если в формулировке какого-нибудь пункта и будет допущена неточность, ее легко устранить, так как формулировка пункта предельно кратка. При этом само исправление уточнит первоначальное восприятие. Иногда полезно составить не один, а несколько вариантов плана или отдельных его частей, особенно при новых обращениях к источнику.

Составляя план при чтении, прежде всего, стараются определить границы микротем текста, т. е. те места, где кончается одна микротема и начинается другая. Эти места в книге тотчас же и отмечают. Нужным отрывкам дают заголовок, формулируя пункт плана. Затем снова просматривают прочитанное, чтобы убедиться, правильно ли установлен переход от одной микротемы к другой, и уточнить, если необходимо, формулировки. При этом нужно стремиться, чтобы заголовки – пункты плана – наиболее полно раскрывали мысли автора. Последовательно прочитывая текст, составляют к нему черновой набросок плана с нужной детализацией. Если план должен стать самостоятельной формой записи, то его обрабатывают в процессе дальнейшего изучения источника.

Правильная работа над книгой окажет тут большую помощь. Чтобы облегчить составление плана, самые важные места в книге отмечают легко стирающимся карандашом или вкладными листками. Подчеркивания, отчеркивания и надписи, выносимые на поля в книге или на листках, станут своеобразными пунктами составляемого плана. Порой эти надписи или подчеркнутые фразы книги и будут записаны как пункты плана.

Подзаголовки книги и оправданное содержанием деление текста на абзацы облегчают создание плана. Однако часто, составляя план книги (особенно когда он предназначен для последующей разработки тезисов), не обращают внимания на подзаголовки, членящие текст, а тем более на абзацы. В этом случае стараются оценить высказывания автора по существу и отобразить их в плане, причем последовательность его пунктов не обязательно должна совпадать с порядком изложения содержания в оригинале, поэтому, в частности, полезно рядом с пунктами плана писать номера страниц относящегося к ним текста.

Способы работы. Иногда в начале работы уже по характеру материала и целям составления плана видно, что он должен быть сложным, но порой это становится ясно не сразу, а лишь в ходе его написания. Составляя сложный план, объединяют часть пунктов под одним заглавием или, наоборот, детализируют некоторые пункты, разбивая их на более мелкие. Другими словами, возможны два способа работы:

1. Составляют подробнейший простой план, а далее преобразуют его в сложный, группируя части пунктов под общими для них заголовками (основными пунктами сложного плана).

2. Составляют краткий простой план и затем, вновь читая текст, пишут сложный,

подыскивая детализирующие пункты. Этот путь, требующий больших затрат времени, приемлем лишь при продолжительной, заранее запланированной работе над фундаментальным произведением.

В общем же случае целесообразно составлять подробный, детальный план к тексту книги при первом же ее чтении. Такой план превратить в сложный, объединяя пункты, выбрасывая мелкие, куда легче, чем вновь обращаться к тексту книги, фактически вторично работая над планом и с текстом. Да и сам процесс обработки детального простого плана помогает лучше разобраться в содержании: ведь, объединяя, обобщают, а выбрасывая, выделяют главное, фильтруют его в своем сознании.

Все пункты плана не обязательно записывать только в вопросительной или только в утвердительной форме. Приемлема как та, так и другая форма. Как правило, пункты плана формулируют по-своему. Но они частично или полностью могут текстуально совпадать с отдельными фразами источника. От этого план лишь выигрывает. Обычно варианты плана могут дополнять друг друга, уточняя и расширяя содержание. Вам не придет в голову писать два–три варианта конспекта, а вот план имеет смысл записывать в вариантах, особенно тогда, когда появляется естественное желание пришедшие в голову удачные, острые формулировки тут же, не откладывая, записать, чтобы не забыть.

Запись планов. Чтобы избежать нерационального переписывания, главные заголовки сложного плана выделяют из подробного простого, подчеркивая часть пунктов. Если сделать этого нельзя, заголовки выписывают в отдельные графы (тем самым как бы вписывают между простыми пунктами). При уплотненной записи заголовки приходится выносить на поля и отсылать стрелкой к нужному месту. Вот почему опытные читатели стараются писать планы с большими интервалами между пунктами и с достаточными для дополнений полями.

Если черновую разработку такой формы записи плана можно рекомендовать как полезную, но не обязательную, то для схематического плана, т. е. плана–схемы, отражающего взаимосвязь пунктов, черновик в большинстве случаев необходим. Иначе не получить полноценной схемы.

Запись любых планов желательно делать так, чтобы ее легко можно было увидеть в целом. Для этого пункты записывают на одном большом листе бумаги (всегда лишь с одной его стороны) или на нескольких листах, но опять-таки не используя их оборота. Тогда, если нужно, читатель сразу сможет увидеть все пункты (листки для этого раскладывают один под другим, чтобы, не переворачивая их, скользить взглядом по всей записи).

Сложный план большого объема полезно записывать в нескольких вариантах. Пример из нашей книги: отдельно выписать основные разделы – чтение, рабочий каталог, записи в библиотеках, техника, а затем полное оглавление, раскрывающее по пунктам подробно все содержание глав. Планы накапливают и хранят:

– в отдельных тетрадях;

– в самом источнике (в этом случае они могут быть записаны на полях, скажем, в газете или приложены на вкладных листках);

– в каталоге (на карточках или на листках, сложенных «гармошкой» в формат

карточек).

Ограниченность применения. Читателю полезно знать о тех недостатках плана, которые ограничивают применение этой формы записи как независимой.

План говорит лишь, о чем сказано в источнике, но не дает сведений о том, что и как сказано, т. е. не передает фактического содержания, а лишь скупо упоминает о нем, о схеме его расположения. Отсюда вывод: планом можно пользоваться, чтобы оживить в памяти хорошо знакомый текст или воспроизвести в памяти слабо запоминающийся текст вскоре после составления плана. Лишь в этих случаях не потребуется вновь обращаться к источнику. Когда же план как форма записи не может выполнить тех задач, которые стоят перед читателем, приходят на помощь другие виды записей: выписки, а также тезисы, конспекты, рефераты.

3.5. Поиск информации

Умственный труд в любой его форме всегда связан с поиском информации. Тот факт, что этот поиск становится сейчас все сложнее и сложнее, в доказательствах не нуждается. Усложняется сама система поиска, постепенно она превращается в специальную отрасль знаний. Знания и навыки в этой области становятся все более обязательными для любого специалиста. Понятие подготовленности в этом отношении складывается из следующих основных элементов:

– четкого представления об общей системе научно-технической информации и тех возможностях, которые дает использование информационных органов своей области;

– знания всех возможных источников информации по своей специальности;

– умения выбрать наиболее рациональную схему поиска в соответствии с его задачами и условиями;

– наличия навыков в использовании вспомогательных библиографических и информационных материалов.

Документальные источники информации. Под «источником научной информации» понимается документ, содержащий какое-то сообщение, а отнюдь не библиотека или информационный орган, откуда он получен. Это часто путают. Документальные источники содержат в себе основной объем сведений, используемых в научной, преподавательской и практической деятельности, и поэтому в этом разделе речь идет именно о них.

Характеризуя документальные источники научной информации, необходимо подчеркнуть их многообразие. Все документальные источники научной информации делятся на первичные и вторичные. В первичных документах и изданиях содержатся, как правило, новые научные и специальные сведения, во вторичных – результаты аналитико-синтетической и логической переработки первичных документов. Оценка документальных источников информации включает в себя такие критерии, как полнота

и достоверность данных, сроки их опубликования, наличие теоретических обобщений и критических материалов, реальность их получения.

Применительно к задачам конкретного поиска каждый из перечисленных источников имеет свои достоинства и недостатки. Не являются здесь исключением даже такие основные их виды, как книги и журнальные статьи. В большинстве случаев любая книга имеет, например, тот недостаток, что за три-четыре года, которые пошли на ее подготовку и издание, содержащиеся в ней данные могли в какой-то степени устареть.

Далеко не идеальным источником информации может считаться и научный журнал. Каким бы узкоспециальным он ни был, тематика его значительно шире, чем конкретные интересы того или иного специалиста, материалы по теме любого произведения всегда рассеяны по громадному количеству журналов.

Такой же неоднозначной будет оценка и всех других документальных источников информации. Важно здесь, однако, видеть не только недостатки, но и те возможности, которые открываются при использовании каждого их вида. Так, в дополнение к широко распространенным журналам необходимо обращаться к различного рода продолжающимся изданиям («Трудам», «Запискам», «Известиям» и т. д.), в которых часто находятся материалы, интересующие самый узкий круг специалистов и отражающие направление деятельности отдельных учреждений.

Нужно помнить о своеобразии такого источника, как труды различных конференций, содержащие сведения о ведущихся исследовательских и опытно-конструкторских работах и их предварительных результатах.

Нужные материалы могут содержаться в специальных технических изданиях, причем некоторые из них, например описания изобретений и авторских свидетельств, содержат не только сведения по определенным техническим устройствам, но могут помочь проследить историю того или иного изобретения или открытия и получить представление о современном направлении научно-технической мысли в какой-то конкретной области.

Информация, содержащаяся в непубликуемых документах, как правило, новее, чем в любых публикациях, и, что очень важно, всегда значительно полнее, так как она еще не подверглась «сжатию», неизбежному при подготовке к печати.

Характеризуя отдельные виды вторичных документов и изданий, также следует подчеркнуть, что все они различны по своему содержанию и назначению. Из сказанного нетрудно сделать вывод: насколько важно знать все документальные источники информации в своей области и уметь выбрать те из них, в которых содержатся необходимые для работы данные.

Организация справочно-информационной деятельности. Приступая к поиску необходимых сведений, следует четко представлять, где их можно найти и какие возможности в этом отношении имеют те организации, которые существуют для этой цели, – библиотеки и органы научно-технической информации.

В первую очередь это библиотеки научные и специальные, т. е. предназначенные для обслуживания ученых, преподавателей и специалистов различного профиля. По своим возможностям они не равны, но формы обслуживания читателей у них в основном одни и те же: справочно-библиографическое; читальный зал; абонемент;

межбиблиотечный обмен; заочный абонемент; изготовление фото – и ксерокопий; микрофильмирование.

Межбиблиотечный абонемент (МБА) представляет собой территориально-отраслевую систему взаимного использования фондов всех научных и специальных библиотек страны. Зная о существовании той или иной книги, но не найдя ее в доступной библиотеке, можно заказать ее по МБА. Присланные на определенный срок книги выдаются для работы в читальном зале.

Органы научно-технической информации. Исходя из задач развития науки и практики, в соответствии с социально-экономической структурой нашего общества создана единая государственная система научно-технической информации (ГСНТИ), включающая в себя сеть специальных учреждений, предназначенных для ее сбора, обобщения и распространения. Предназначена она для обслуживания как коллективных потребителей информации – предприятий, научно-исследовательских и проектно-конструкторских организаций, – так и индивидуальных.

В основу информационной деятельности в нашей стране положен принцип централизованной обработки научных документов, позволяющий с наименьшими затратами достигнуть полного охвата мировых источников информации и наиболее квалифицированно их обобщить и систематизировать. В результате этой обработки подготавливаются различные формы информационных изданий.

Непосредственную помощь специалистам в поиске информации оказывают отделы (бюро) научно-технической информации в научно-исследовательских и проектных институтах и на предприятиях. Работа каждого из них строится с учетом информационных потребностей учреждения в целом и отдельных категорий специалистов.

В соответствии с ними формируется справочно-информационний фонд (СИФ), состоящий из массива информационных документов и справочно-поискового аппарата, включающего в себя, помимо традиционных указателей и каталогов, различные картотеки: отчетов о выполненных научных исследованиях, проектной документации, авторских свидетельств и патентов, стандартов и нормалей, выпускаемых изделий, материалов, комплектующих деталей, узлов и аппаратуры, переводов, микрофильмов и т. д.

Библиографические указатели. Рост научной и технической литературы делает очень важной проблему «ключа» к ней. Таким ключом служат библиографические указатели – перечни литературы, составленные по тому или иному принципу. Библиография растет сейчас такими же быстрыми темпами, как и объем печатной продукции. Только в нашей стране ежегодно выпускаются тысячи названий различных библиографий и ряд специальных периодических изданий библиографического характера. Подготовкой различного рода библиографических изданий занимаются многие организации: книжная палата, крупные библиотеки, институты научно-технической информации, многие научные учреждения и учебные заведения. Помимо тех библиографических указателей, которые выпускаются в виде отдельных изданий, библиография в той или иной форме присутствует в большинстве книг и статей. Все это определяет исключительное многообразие библиографических указателей. Они могут быть самыми различными по своим задачам, содержанию и форме.

Многообразие библиографических источников делает обязательным для любого специалиста иметь представление о всех их видах, как специальных (отраслевых), так и общих. Здесь приводится характеристика только некоторых основных изданий текущей библиографии.

Следить за всем тем, что выходит в стране, позволяет, прежде всего, комплекс «Летописей», издаваемых Книжной палатой. Сведения о книгах и брошюрах по всем отраслям знаний содержит «Книжная летопись». В основном ее выпуске, выходящем еженедельно, приводятся данные о научной, научно-популярной, производственной и художественной литературе, а также о продолжающихся изданиях типа «Трудов» и «Ученых записок». В дополнительном выпуске (издается раз в месяц) описываются ведомственные, инструктивно-производственные, нормативные, учебно-методические и информационные издания, книги, вышедшие без цены и бесплатно. Авторефераты диссертаций выходят отдельным выпуском.

Наряду со специальными библиографическими изданиями, основным содержанием которых являются сведения о различных произведениях печати, информацию о литературе дают многие книги и периодические издания. Эта информация составляет их библиографический аппарат, именуемый прикнижной (пристатейной) библиографией. Она рассматривается как составная часть библиографии определенной области или научной дисциплины.

Приведенный обзор касался главным образом общих и универсальных текущих показателей. В дополнение к ним каждый специалист непременно должен иметь подробный перечень всех библиографических изданий своей отрасли знаний, своей специальности и по всем проблемам, которыми он непосредственно занимается. Ориентироваться в них надо настолько свободно, чтобы безошибочно обращаться к тем из них, где наиболее целесообразно искать материалы по интересующему вопросу.

Последовательность поиска документальных источников информации. При описании каталогов, картотек, библиографических указателей и информационных изданий все время подчеркивалось, насколько важно иметь исчерпывающее представление о всех их видах и стараться использовать их как можно полнее. Однако нельзя понимать это как универсальный совет и по любому случаю обращаться ко всем библиографическим источникам одновременно. При их большом количестве и многообразии дело это совершенно нереальное.

Во всех руководствах рекомендуется выбрать те из них, которые в наибольшей степени соответствовали бы конкретным задачам поиска. Такая рекомендация совершенно правильна, но сам термин «выбрать» нуждается в некотором уточнении. О выборе чаще всего говорят, когда дело идет о многообразии чего-то, в основном однородного.

В отношении библиографических источников все обстоит значительно сложнее. Здесь можно видеть не простое многообразие, но наличие определенной иерархии по степени их полноты, сложности. Кроме того, все они определенным образом взаимосвязаны друг с другом. Не случайно говорится о системе библиотечных каталогов и библиографических указателей. Здесь термином «система» как раз и подчеркивается их взаимосвязь. Естественно поэтому предположить, что и использование их также должно быть подчинено какой-то системе. Значит, правильнее говорить не о выборе библиографических пособий, а о той последовательности, в

которой должен идти поиск документальных источников информации. На этом основании допустимо считать, что заведомо неверным является поиск, ведущийся путем «сплошного» просмотра всех имеющихся библиографических материалов. Практика полностью это подтверждает.

Бессистемный поиск всегда отнимает непомерно много времени и одновременно не дает гарантии его полноты. Между тем, как это ни странно, даже опытные специалисты редко задумываются над тем, насколько рационален их путь в поисках нужной информации.

Цели и условия поиска документальных источников информации настолько различны, что никакой единой схемы быть не может. Необходимость своей особой схемы поиска наглядна уже при одном перечислении тех целей, которые при этом могут преследоваться: в одном случае требуется установить полный перечень литературы по определенной теме, в другом – только наиболее современные или главнейшие публикации по той или иной проблеме; для одних работ требуется добраться до первичных источников информации, для других достаточно информации, содержащейся во вторичных документах, и т. д.

Подход к поиску литературы может зависеть и от того, в какой последовательности ее предполагается изучать: в хронологической, когда литературные источники рассматриваются в их прямой хронологической связи, или обратнохронологической, когда знакомятся сначала с новейшими изданиями, а затем уже переходят к более старым по времени публикациям. Совершенно очевидно, что в каждом случае будут совсем различными и сам перечень библиографических материалов, и последовательность обращения к ним.

Хорошо ориентируясь в библиотечных каталогах и библиографических указателях, можно без особого труда составить схему поиска документальных источников информации применительно к его конкретным целям.

3.6. Методы изучения документов

Классические методы. *Исторический метод* ставит проблему валидности в трех аспектах: 1) Подлинность текста и установление его автора. Исследователь должен быть уверен, что документ является именно тем, каким он его принимает, и действительно принадлежит далекому автору. Такая подлинность устанавливается по характеристикам документа: материальным признакам – бумага, почерк и т. д. или признакам формы – тон, стиль, словарь. 2) Валидность интерпретации текста, его значение по отношению к автору текста, по характеру, целям, которые он преследует. 3) Правдивость фактов, изложенных в документе. Первый и третий аспекты, то есть подлинность и правдивость, особенно важны для исторического метода. Но применяться он может и при изучении литературного или юридического текста.

Литературный метод выявляет подлинность текста и автора, изучая тон, стиль и словарь. Устанавливается, например, что автором такой-то пьесы не мог быть Шекспир.

Психологический метод более индивидуален, позволяет исследовать характеры, как самих авторов, так и изображаемого ими, соотносит героев с социальным контекстом, который их породил. Объяснение может быть психоаналитическим, экзистенциалистским и т. д. в зависимости от школы, к которой принадлежит исследователь.

Юридический метод применяется при изучении текстов или судебной практики, он позволяет сравнивать тексты, исследовать мотивы решения, цели законодателя и т. д.

Социологический метод объясняет документ в его социальном контексте.

Лингвистический метод за последние годы шагнул далеко вперед и еще не исчерпал всех своих возможностей. По времени возникновения он может быть отнесен к числу классических, однако его специфичность и особенности эволюции в последнее время ставят этот метод особняком и весьма сближают с современными и структурными методами. Например, задачи лингвиста в основном состоят в выявлении минимальных единиц языковой системы, фонемы и морфемы, а также в исследовании последовательности и сочетаний этих единиц. Лингвиста интересует не значение текста, а его структура, другими словами, распределение морфем и фонем. Наконец, лингвист наблюдает наличие или отсутствие определенных лингвистических единиц, а также частоту их употребления. Таким образом, можно подойти к проблеме возможного, значения распределений и структур.

Так называемые классические методы, кроме лингвистического анализа документов, имеют много общего, хотя они могут быть не только рациональными (юридический анализ), но и в определенной степени интуитивными, личными, субъективными. Качественный элемент является здесь основным, а то, что может исчисляться количественным путем, воспринимается только интуитивно и нерасчлененно.

Такие виды анализа имеют дело с различными случаями несистематизированного творчества, ценность которого зависит только от его исполнителя. Количественный рост средств коммуникаций (радио, телевидения) и пропаганды увеличивал потребности в поиске значений, корреляций, закономерностей в оценке факторов влияния и предвидении некоторых событий. Современный метод анализа документов возник из необходимости проводить исследования в новых направлениях.

Контентный анализ. Данные, которые нам представляют социальные науки, состоят в основном из сообщений – устных (тексты речей, записи бесед, разговоры) или письменных (официальные документы, газетные статьи, письма, в том числе литературного, исторического и политического содержания).

Независимо от уровня и исследуемого материала, независимо от того, хотим ли мы понять или объяснить мнение, поведение, действие, данные, получаемые нами, почти всегда выражены в словесной форме. Всякое фиксируемое нами действие облачено в словесный контекст. Важно, чтобы исследователь в социальных науках мог научно анализировать эти материалы, не довольствуясь только простыми впечатлениями.

Литературные и исторические анализы текстов сохраняют свою ценность, однако их могут дополнить современные методы. Новизна современных средств контентного анализа заключается в том, что впечатления исследователя, которые зависят от его личных качеств, заменяются более стандартизованными процедурами, которые часто предполагают измерение и, во всяком случае, выражают материал в виде данных,

которые могут рассматриваться научно. Для этого необходимо расчленить текст, иными словами, исследовать его, исходя из функций отдельных понятий или слов, которые выбираются и учитываются в зависимости от целей исследования.

Требования к контентному анализу. *Объективность*. Анализ должен подчиняться достаточно ясным и точным правилам, чтобы разные толкователи, работая с одним и тем же текстом, получали одинаковые результаты. Это предполагает возможность договориться по всем аспектам анализа, добиться одинакового понимания всех категорий и рабочих определений каждой из них. *Систематичность*. Все содержание должно быть упорядочено и интегрировано в категориях, избранных в зависимости от преследуемой цели. Никакие элементы информации, имеющие отношение к цели, не должны остаться вне поля зрения. *Измеримость*. Чаще всего речь идет о перечислении значимых элементов, о подсчете их частоты и т. д. Но эти условия не всегда соблюдаются, иногда применяются и приемы качественного анализа к проблемам, которые не подлежат измерению. Контентный анализ может охватить:

1) Все данные словесного сообщения, которое имеет значение в общественной жизни, идет ли речь о текстах письменных (официальные документы, книги, газеты, личные документы) или устных (радио, телевидение) или о деятельности, поддающейся расчленению и классификации (анализ совещания, расписание рабочего времени мастера или префекта).

2) Все данные, специально полученные социально-психологическим исследованием (отчеты о беседах, дискуссии в группах и т. д.).

Типы контентного анализа:

1. *Поисковый и контрольный анализ.* Направленный и ненаправленный анализ. Сначала подчеркнем существенную особенность, свойственную всем исследованиям в общественных науках: различие между анализом документов, направленным на проверку определенной гипотезы, анализом, цель которого точно выражена, ясно, что исследуется и где квантифицируется результат, и таким анализом, цель которого нужно найти. Очевидно, что первый тип анализа более точен и более систематичен. Если исследователь хочет классифицировать некоторые значимые элементы документации так, чтобы получить количественное их определение, он должен либо знать то, что он хочет высчитать, либо действовать интуитивно, отказываясь от любой систематизации. Если количественный контентный анализ применяется к большому числу данных без четких гипотез, то исследователь тратит впустую свое время и силы. С целью систематизации следует применять направленный анализ, хотя надо признать и его неудобства: возникает опасность, что в поле зрения исследователя не попадут существенные элементы, которые он не предвидел.

2. *Количественный анализ и качественный анализ*. Слово «качественный» долгое время исключалось из контентного анализа. Авторы противопоставляли понятия качественного и количественного, исходя из разных точек зрения: впечатление они противопоставляли систематизации, гипотезу – проверке гибкости или жесткости категории. Качественный анализ учитывает наличие или отсутствие данной характеристики, тогда как количественный анализ рассматривает частоту отдельных тем, слов, символов, содержащихся в тексте. С помощью количественного анализа, правда, можно рассматривать и наличие или отсутствие определенных атрибутов, но основное внимание обращается на частоту их применения и на основе этого делаются

выводы. Постараемся также выяснить различие между двумя типами анализа с точки зрения критерия «важности». В количественном анализе таким критерием является число случаев; здесь важно нечто часто встречающееся. В качественном же анализе «важность» предполагает новшество, занимательность, ценность данной темы, так что критерий важности остается явно субъективным. Количественный подход, обладающий бесспорным свойством объективности, ограничен тем, что не принимает во внимание редко встречающиеся темы и символы или игнорирует их оригинальность, относя к более общим группам. Исследователь теряет ценную информацию, если он произвольно применяет категории анализа и выборку, удовлетворяющую техническим требованиям статистического анализа. Исследователь же, интересующийся ценностью самих показателей, постарается получить более узкие категории, тем самым превращая их в специфические, лучше приспособленные для изучаемой данной действительности. В любом реальном анализе существуют две опасности: принять узкие категории, хотя и соответствующие реальности, но отражающие ее в темах слишком узкого диапазона, или же сгруппировать данные в небольшое число категорий, отказавшись от ряда оригинальных черт этих данных.

3. *Непосредственный или косвенный анализ*, репрезентативная и инструментальная коммуникация. При количественном анализе измерение чаще всего применяется в прямой форме. Исходя из количественного анализа, можно, однако, более тонко интерпретировать то, что, в частности, скрыто присутствует в языке. Косвенная интерпретация, то есть выявление некоего подтекста сказанного, не является достоянием лишь качественного анализа; она вполне может исходить из квантификации содержания. Чаще всего квантификация содержания довольствуется представлением результатов в цифрах, и поэтому изменение стратегий, кажущаяся бессвязность содержания заставляют искать объяснение гипотезы в той области, которая скрыта и неопределима количественно. Прямой количественный анализ ограничивается подсчетом ответов в таком виде, в каком они даны. Косвенным количественным анализом можно обнаружить и то, что не является очевидным, даже то, что автор текста хотел умышленно скрыть. Недомолвки, темп и ритм речи, выбор слов в тексте – все эти формальные признаки могут раскрывать очень многое, поскольку автор сообщения не следит сколько-нибудь сознательно за этим и не замечает их информативной ценности. Эти признаки являются ценными показателями, касающимися автора сообщения, особенно когда речь идет об инструментальной коммуникации, то есть коммуникации, предназначенной произвести определенный эффект на реципиента сообщения (напротив, чисто репрезентативная коммуникация информирует о состоянии коммуникатора).

4. *Структурный анализ.* Двусмысленность самого термина «структура» позволяет применять структурный анализ в исследованиях разных типов.

Категории анализа должны соотноситься со структурами данных и единиц, связанных с включенными в объект исследования гипотезами.

Употребление контентного анализа. Изучение коммуникации в рамках схемы «коммуникатор – реципиент». В любом виде коммуникации существует коммуникатор, который отправляет сообщение, имеющее содержание и форму. Такое сообщение передается с целью быть принятым, оно обращено к одному или многим реципиентам. Это выражается в краткой схеме: кто говорит? что говорит? как? кому? с каким результатом? В зависимости от конкретного случая можно изменять порядок этих

вопросов, которые фактически охватывают всю совокупность проблем. С помощью контентного анализа можно, следовательно, изучать:

Кто говорит? Исследование коммуникатора. Тут возможны два случая. В первом отправитель реагирует на стимул, более или менее контролируемый наблюдателем: например, беседа, которую ведет психотерапевт. Чаще встречается другой случай, когда исследователь не имеет никакой связи с коммуникатором и по содержанию передаваемой информации, по письмам или произнесенным речам судит о характеристиках коммуникатора.

Что говорит? Речь идет об исследовании содержания передаваемого сообщения.

В общем плане исследование широкой публики при большом количестве тесно взаимосвязанных факторов связано с некоторыми трудностями. Индивид реагирует на получаемое сообщение, касающееся крупных социальных проблем, в зависимости от системы общественных ценностей воспринятых им через повседневность и, так сказать, приспособленных к потребностям его личности, которая в свою очередь приспосабливается к своей среде. Совокупность фактов, полученных эмпирическим путем, можно объяснять с помощью как общих, так и частных теорий социальной психологии, в которой понятия мотивации и референтной группы играют все более важную роль. Коммуникатор менее изучен, так как исследователей больше интересовала проблема влияния массовых коммуникаций на аудиторию. Более современные работы по контентному анализу направлены на изучение связи между коммуникатором и реципиентом. Эта связь рассматривается в широком социальном контексте, содержащем значительное количество взаимодействий, которые не поддаются расчленению. Последние влияют на коммуникатора, реципиента и, сверх того, на тех, кому сообщение было передано косвенным образом. Исследователь имеет дело с огромной сетью коммуникаций, которую он может наблюдать только фрагментарно и не в состоянии пока полностью воспроизвести. Несмотря на эти трудности, проблема больше не ставится на уровне связи коммуникатор – реципиент. Она рассматривается в более широком кругу социальных отношений, затрагивая такие вопросы, как столкновение разных форм коммуникации: личных, устных аудиовизуальных, местных и национальных, изучается зависимость эффективности коммуникации от условий, темы, типа общества и т. д.

Технические стадии контентного анализа. В любом исследовании на первом этапе определяется предмет и цель работы. Чтобы получить ответ, надо поставить вопрос. При интервьюировании беседа строится на основе вопросника, при анализе документов исследователь исходит из категорий, которые он усматривает в данных документа. Если цель уточнена, выбор категорий составляет первую стадию техники контентного анализа в собственном смысле.

1. *Первая стадия – выбор категории.* Формулирование категорий. Категории являются значимыми рубриками, согласно которым квалифицируется, а возможно, и квантифицируется содержание. Поскольку речь идет о результатах анкетирования, принятые заранее категории создают определенный код. Может быть два случая.

В первом, когда исследователь хочет проверить гипотезу, категории принимаются заранее. Так, при изучении мнения с помощью интервью предварительный опрос позволяет дать некоторую классификацию ответов: очень нравится, не очень нравится и т. д. При верификации гипотезы в исследовании документов также действует

заранее составленный вопросник.

Во втором случае имеет место перечисление элементов содержания без предварительной гипотезы и категории предварительно не устанавливаются. Надо просто установить некоторый перечень разных мнений или использованных аргументов.

Можно также поставить перед собой более сложную и широкую задачу при анализе документов или психологических интервью. Контентный анализ здесь должен выявить неизвестные переменные и факторы. Обнаруженные и учтенные темы и установки должны указать направление исследования и объяснения скрытого содержания.

При отсутствии исходной гипотезы подбор категорий усложняется. Он должен исходить из самого содержания, быть как можно меньше ориентированным. Следует несколько раз проанализировать текст, чтобы выявить существенное в соответствии с целями исследования содержание.

При поисковом опросе категории образуют рамки анализа. С их помощью отбираются данные. Не следует торопиться при их определении, чтобы не пропустить данных, важность которых может обнаружиться позднее с помощью более разработанных гипотез.

Характеристика категорий. Основным в контентном анализе является выбор категорий. Они образуют связь между целями исследования и его результатами. Как выразился Берельсон, «контентный анализ стоит столько, сколько стоят его категории». Необходимо различать технические возможности, которые могут дополнять категории, повышая ценность анализа и такие качества, как проницательность и тонкость, зависящие от опыта, интуиции, знакомства исследователя со средой. Мы здесь акцентируем внимание только на технических свойствах категорий. Они должны быть, прежде всего, исчерпывающими, то есть пригодными для рассмотрения всего содержания. Конечно, можно при желании обойти некоторые аспекты содержания и в соответствии с поставленной целью решить, что именно следует квалифицировать. Категории должны обладать признаком исключительности: одни и те же элементы не должны принадлежать к нескольким категориям. Так, на вопрос, где проводилась беседа, в одной анкете были предусмотрены следующие категории ответа: «на работе», «дома», «в кафе». А как, например, классифицировать крестьян, для которых ферма является одновременно домом и местом работы? Иногда приходится закодировать индивида в нескольких категориях, например, когда изучается, на каких иностранных языках говорят опрашиваемые.

Категории должны быть объективными, их характеристики должны быть ясными для разных кодировщиков, чтобы они могли классифицировать разные элементы содержания с помощью одинаковых категорий. Категории должны быть уместными, соответствуя преследуемой цели и исследуемому содержанию. Если категории предвидятся заранее, возникает опасность пожертвовать их уместностью. На деле категории должны проистекать из двух источников при анализе документов – из самого документа и из некоторых общих знаний в области, которую он раскрывает. При анкетном опросе – из ответов или из целей, замыслов, значений коммуникатора, если речь идет о тексте. В зависимости от ситуации принимаются во внимание и отсутствующие элементы, которые могут быть значимыми.

Рамки соотнесения. Уместность заключает в себе важное условие общего порядка, особенно когда речь идет об опросе с помощью интервью. В эмпирическом плане очень важно приспособление рамок анализа и его категорий к возможностям опрашиваемых и к самой ситуации опроса.

Трудности. Нужно стараться избежать следующих четырех крайностей. Принятия априорной слишком жесткой схемы, не соответствующей сложности содержания, или же поверхностной разработки схемы, учитывающей только явные элементы коммуникации, без связи с более или менее скрытым латентным ее содержанием. Выбора слишком многочисленных и слишком дробных категорий, почти повторяющих текст, под предлогом ничего не пропустить или выбора слишком укрупненных категорий, не учитывающих необходимых различий среди группируемых элементов. Надо, наконец, установить уровень измерения изучаемого объекта. Этим определяется зачастую и тип самих категорий. И на этой стадии категория должна подчиняться задаче: она должна обладать значением по отношению к выдвинутой гипотезе и поставленной цели.

Стандартизация. Несмотря на возможное разнообразие задач и тем анализа, некоторые типы категорий встречаются достаточно часто. Для облегчения проведения анализа и сравнений предлагались категории, которые подходили бы для многих случаев. Нельзя дать единый ответ на вопрос о стандартизации категорий в контентном анализе. Во всяком случае, схемы анализа должны подходить как к общей и всеми принятой концептуальной системе, так и к специфическому содержанию, меняющемуся с каждым новым исследованием. Стандартизованные категории могут представлять и удобства, и неудобства – в зависимости от случая.

Чаще всего из-за отсутствия надежной системы, которая помогла бы свести в одно целое различные взгляды, исследователи продолжают интуитивно подбирать категории по своему усмотрению. Кроме такой произвольной стандартизации существуют области, в которых возможна постоянная стандартизация, например, если речь идет об интенсивности коммуникации, об оценке самого сообщения.

Типы категорий. Обратимся к широко употребляемой категории, отвечающей на вопрос: о чем говорит данная коммуникация? Очень часто этот вопрос возникает при определении места какой-нибудь темы в библиотечной классификации, списке сочинений или газетных рубриках. Направление коммуникации соответствует категориям, которые весьма часто употребляются в изучении мнений: за, против, нейтрально.

Ценности. Категория ценностей объясняет или направление коммуникации, или цели, которые она преследует. Среди категорий ценности встречаются такие, которые выявляют то, что опрашиваемые считают признаком успеха: деньги, социальное положение, семья, автомобиль и т. д. Или же такие ценности, которые упоминаются в иллюстрированных журналах, – любовь, деньги, героизм, риск и т. д.

Средства. Категория может также указать средства, которые предлагаются для приобретения данных ценностей. Исследуемые речи, например, могут содержать угрозу, убеждение, насилие, переговоры.

Деятели. Можно постараться выяснить некоторые индивидуальные черты исторических или литературных персонажей или просто анкетируемых лиц. Здесь мы

встречаемся с классическими категориями: возраст, пол, профессия, вероисповедание, национальность, уровень образования, которые дополняются, естественно, в зависимости от поставленной цели исследования. Можно изучать, к какой группе принадлежат интересующие нас лица.

Происхождение. Представляется возможным классифицировать историческую документацию по ее источникам, а исследование избирательной кампании – по речам, объявлениям, листовкам, газетам; газетные сообщения могут разделяться на местные, национальные, международные.

Вышеуказанные категории касались содержания, но имеются также категории, относящиеся к форме. Конкретный пример контентного анализа. Две важные проблемы, соответствующие двум этапам анализа.

1. Какие категории следует выбрать? На какой основе собирать данные? Что мы хотим узнать?

2. Как квалифицировать данные? Какие категории следует выбрать. Весьма скоро обнаружилось, что интерес к референдуму выражается в числе «да» и «нет». Можно было также выбрать из газеты аргументы в пользу «да» и в пользу «нет». Эти категории оказались довольно примитивными, поскольку крайне правые и крайне левые голосовали «нет», и степень убежденности тех, кто отвечал «да», оказалась далеко не одинаковой. Кроме того, некоторые политические группы призывали воздерживаться от участия в голосовании или требовали отменить референдум, а ряд газетных статей содержал комментарии без указания позиций.

Чтение газет и размышления натолкнули нас на выбор категорий направления (коммуникаторы надеются на то или другое) и подкатегории интенсивности: энтузиаст, умеренный. Эти категории, как нам показалось, соответствуют техническим требованиям. Они – объективные (даже различение между «да» энтузиаста и «да» умеренного не поднимало трудно объяснимых вопросов, и обе группы кодировщиков получили одинаковые результаты), исчерпывающие, уместные, взаимоисключающие. В связи с последней категорией возник ряд вопросов.

Если целая статья в рубрике «Открытая трибуна» излагает аргументы против референдума, но кончается призывом голосовать «за», то, как рассматривать цель всей статьи? Этот случай имеет отношение к проблеме квантификации, которую мы и рассмотрим.

2. *Вторая стадия: вопросы квантификации содержания.* Цель анализа заключается в квантификации выбранных при помощи указанных категорий позиций по отношению к референдуму, содержащихся в разных рубриках газеты. Анализ осложнялся следующими обстоятельствами.

1. Кампания продолжалась тридцать дней, и поэтому пришлось изучать 30 номеров газеты.

2. Каждый номер газеты содержал разные рубрики; передовую статью, отражающую направленность газеты, независимые выступления, информацию.

3. В защиту каждой позиции, «да» или «нет», использовались иногда сходные аргументы, но с разными целями.

Нужно ли учитывать все номера газет или сделать выборку? Если выборку, то какую? В каком объеме требуется квантификация? Надо ли различать статьи (в том числе по признаку «да» и «нет»)? Какие еще единицы надо подсчитывать? Считать ли количество слов «да» и «нет», считать ли количество строк или сантиметров текста, посвященного этим позициям?

К основным проблемам квантификации контентного анализа относятся:

1) *Проблема выборки.* Первые контентные анализы страдали от отсутствия методики при выборе источников: иногда стремились рассматривать все тексты, иногда изучали ряд речей и т. д. Что может обеспечить репрезентативность выборки документов? Заранее это неизвестно. Чаще всего признаки определяют в зависимости от формулируемых гипотез; это, однако, малонаучно и может не учитывать всех факторов. Проблема выборки содержит в себе три решения, если речь идет об анализе коммуникации: выбор источника, число и дата сообщений, исследуемое содержание.

2) *Выбор источника.* Этот выбор зависит от задачи. При изучении прессы можно сделать географическую выборку, учитывающую роль местных газет. Если речь пойдет о сравнении разных аудиторий читателей на основе анализа романов, печатаемых в журналах и читаемых в разных кругах, изучаемая совокупность будет состоять из всех романов, печатаемых во всех журналах, вышедших в стране за какое-то определенное время. Но можно провести и репрезентативную выборку этих журналов, а также выборку романов из каждого журнала. В данном случае мы сталкиваемся со сложной проблемой репрезентативной выборки. Можно ли считать репрезентативным роман, если журнал, в котором он публикуется, имеет небольшое число читателей или страниц? Публикует ли данный журнал лишь этот или несколько романов? Если исследователь в состоянии подтвердить общие выводы, которые он сформулировал на основании изученных данных, он должен суметь точно выразить мотивы, которые побудили его ограничить изучаемую совокупность.

3) *Число сообщений и временной диапазон.* Чтобы выборка была достаточно репрезентативной, нужно установить затем, каково должно быть число сообщений и какой период времени они должны охватывать. Время зависит от избираемой темы. В частности, речь может идти о послевоенном периоде или о впечатлении от определенных речей за три месяца. Нужно, чтобы изучаемая единица с определенной вероятностью попадала в выборку и в то же время была независимой от любых корреляций между единицами этой совокупности. Представим, что мы решили ограничиться выборкой одного номера данной газеты из семи. Что мы должны делать, если выбор падает на воскресный выпуск, который значительно отличается от других? Необходимо заранее отметить периодические отклонения выбранных источников, которые могут влиять на характер сообщений.

4) *Наблюдаемое содержание.* Остается, наконец, определить выборку выборки, то есть установить наблюдаемое содержание изучаемой газеты за конкретный период. Содержание должно соответствовать свойствам газеты, которые зависят от типографии, от расположения и т. д. Так, первая страница газеты отличается от последней.

5) *Разные единицы квантификации.* При квантификации надо выбрать постоянные признаки категорий и установить величину элементов, на которые расчленяется

содержание.

6) *Единица регистрации.* Первой единицей анализа является единица регистрации. Это определенный сегмент содержания, который характеризуется при введении его в определенную категорию. Единицы регистрации являются переменными величинами. Слово – мельчайшая единица. Можно подсчитать, сколько раз в тексте употреблялись определенные слова. Например, в анализе политического текста, содержащего такие категории, как «национализм» и т. д., слова «родина» и «нация» могут причисляться к единицам регистрации в категории «национализм». Тема – это значимый фрагмент, соответствующий идее, которая охватывает одну из категорий. Вместо того чтобы ограничиться словом «родина» в предыдущем примере, можно взять тему, например, «демократия». Тема – элемент менее точный, чем слово, так как она может занимать две строчки или страницы. Можно удовлетвориться числом повторяющихся упоминаний темы, как и числом повторяющихся слов. Но не будет ни точным, ни соответствующим действительности равно учитывать краткое упоминание и пространное изложение темы. Понятно, что, кроме единицы регистрации, которая представляет элемент, иллюстрирующий данную категорию, требуется еще более гибкая и точная единица измерения, чем число повторений. Ниже мы встретимся с такой единицей, которая называется единицей перечисления.

7) *Предмет.* Этот, несомненно, наиболее употребляемый термин в широком смысле слова означает содержание целиком – книги, фильма, речи. В узком смысле «предмет» может быть синонимом единицы регистрации, то есть всего того, что подвергается измерению. Слово, тема, вопрос, употребленные в смысле единицы регистрации, рассматриваются просто как предметы.

8) *Единица контекста.* Это более гибкое понятие, не предполагающее строгой квантификации. Это лишь более широкий сегмент содержания, к которому мы обращаемся, чтобы понять саму единицу регистрации. Например, если единицей регистрации является слово, то единицей контекста может быть предложение.

9) *Единица перечисления.* Здесь речь идет не о значении, которое надо подсчитать, а о способе самого подсчета. Другими словами, если установление единицы регистрации преследует цель – на что указывает само это понятие – выделения значимого элемента, то единица перечисления касается способа перечисления разных выделенных частей.

Если мы хотим выявить разницу между двумя темами, одна из которых встречалась десять раз в строке, а другая – один раз в пятидесяти строках, необходимо иметь единицу перечисления (число строк), которая бы отделялась от единицы регистрации (число упоминаний темы

Единицы перечисления имеют отношение к пространству или времени: параграф, строка, сантиметр, минуты регистрации. Они должны поддаваться объективному, надежному и проверяемому измерению, должны подвергаться математическим операциям, начиная с самого простого – сложения. Разница между единицей регистрации и единицей перечисления является существенной.

Глава 4. Оформление и использование аналитических результатов

Любые результаты аналитического исследования деятельности предприятия в целом или его сегментов должны быть оформлены соответствующими документами. Это может быть аналитический отчет (пояснительная записка), справка, заключение. Аналитический отчет обычно составляется для внешних пользователей. Если результаты анализа предназначены для внутрихозяйственного использования, они оформляются в виде справки или заключения.

Содержание аналитического отчета должно быть достаточно полным. Прежде всего он должен содержать общие вопросы, отражающие экономический уровень развития предприятия, условия его хозяйствования, характеристику ассортиментной и ценовой политики, конкурентоспособности продукции, широту и долю рынков сбыта продукции, репутацию предприятия, его имидж в деловом мире. Необходимо также указать положение товаров на рынках сбыта, т.е. на какой стадии жизненного цикла находится каждый товар на рынке (внедрения, роста и развития, зрелости, насыщения или спада). Следует охарактеризовать реальных и потенциальных конкурентов, указать сильные и слабые стороны их бизнеса.

После этого необходимо отразить динамику показателей, характеризующих производственные и финансовые результаты, имущественное и финансовое состояние предприятия, его деловую активность, эффективность работы, перспективы развития.

Содержание справки или заключения по результатам анализа в отличие от пояснительной записки может быть более конкретным, акцентированным на отражении недостатков или достижений, выявленных резервов, способов их освоения. Здесь может быть опущена общая характеристика предприятия и условий его деятельности.

Отдельно следует остановиться на бестекстовой форме представления результатов анализа. Она состоит из постоянного макета типовых аналитических таблиц, графиков и не содержит пояснительного текста. Аналитические таблицы и графики позволяют систематизировать, обобщить изучаемый материал и представить его в пригодной для восприятия форме.

Такой порядок оформления результатов анализа в последнее время находит все большее применение. Он рассчитан на высококвалифицированных работников, способных самостоятельно разобраться в обработанной и систематизированной информации и принимать необходимые решения. Бестекстовый анализ повышает его действенность, так как при этом сокращается разрыв между выполнением анализа и использованием его результатов.

Возможные *компоненты аналитической записки*:

1. Введение: указание причин появления документа, изложение основной идеи документа.

2. Основная часть: указание источников сведений, указание степени достоверности сведений, констатация положения в некоторой области, оценка положения, представление и оценка прогноза.

3. Заключение: обобщения, рекомендации, указание возможности и условий улучшения качества представленных сведений, намерения.

Формулирование выводов. Выводы не всегда возможны или уместны:

- иногда для них недостаточно информации;

- иногда они слишком неприятны для читателей и поэтому опасны для разработчика документа;

- иногда они слишком просты и очевидны;

- иногда не желательно мешать читателю поискать еще одно объяснение фактам, которое может оказаться более удачным, чем то, что пришло в голову разработчику документа.

Одни и те же обстоятельства можно обоснованно представить и как существенные, и как не заслуживающие внимания. База, которую можно использовать при оценивании:

- аналогичные случаи;

- принципиальные возможности;

- преследуемые цели.

Степень определенности формулировок должна соответствовать степени определенности стоящих за ними представлений. Правда, чем меньше определенность формулировок, тем меньше возможность ошибок (а следовательно, опасность наказания), но зато снижается полезность выраженных в них мнений как для дела, которого они касаются, так и для репутации аналитической службы.

Неопределенность представлений может быть вызвана неопределенностью отражаемых сущностей: нечеткостью их устройства, зависимостью от многих случайных влияний; чрезмерной сложностью отражаемых сущностей; недостаточными возможностями для исследования.

Неопределенность формулировок может быть вызвана неопределенностью выражаемых ими представлений; осторожностью авторов; неудачностью стиля: различиями в смысле, вкладываемом разными людьми в одно и те же слова; нежеланием авторов делиться информацией.

Аналитики, склонные высказываться определенно о неопределенном, производят впечатление людей проницательных и знающих. Тем, кто к ним прислушивается, они дают уверенность в понимании ситуации, чувство превосходства над «не знающими» и способность действовать. Что же касается получаемых результатов деятельности, то они часто бывают неоднозначные (и соответственно толкуемые как угодно), а иногда даже почти такие, как надо. Но подобные аналитики способны оказывать значительное влияние лишь в течение сравнительно короткого времени – до того, как совершат одну-две большие ошибки, которые при их подходе довольно вероятны. Правда, когда этих аналитиков заменяют на других, то обычно, вследствие тяги к определенности, выбирают работающих в той же манере, и цикл повторяется – пока

заказчик не осознает свою неправоту или пока на его месте не окажется другой.

В числе трудностей, с которыми сталкивается аналитик при формулировании обобщений и рекомендаций, – проблема интеллектуальной ограниченности и недостаточной компетентности людей, которым предназначается материал, и проблема идеологических расхождений аналитика с этими людьми. Результат его работы нередко представляет собой компромисс между тем, что он хотел сказать, и тем, что он мог позволить себе сказать, чтобы не предстать в глазах руководства нежелательным человеком.

Для сложных проблем, с которыми сталкиваются высшие руководители, бывают возможны эффективные радикальные решения, но главное препятствие для реализации таких решений состоит в неспособности руководителей оценить их по достоинству. В очень многих случаях на руководящих должностях оказываются люди, отличающиеся не творческими способностями, порядочностью и самоотверженностью, а умением интриговать и приспосабливаться, склонностью к злоупотреблениям, готовностью делать большие и малые подлости.

Чтобы оказаться востребованным такими людьми, аналитик должен ориентироваться на их понятия и потребности. Нередко бывает, что аналитическая служба может только предполагать, в связи с каким готовящимся решением истребуют у нее те или иные материалы. Возможно даже, что решение уже по сути принято, и дополнительные сведения нужны единственно для его конкретизации. В таком случае разработка каких-либо рекомендаций является пустой тратой времени, а высказывание их может вызвать недовольство. Поэтому, чтобы не делать лишнего, надо по возможности заранее оговаривать с заказчиком аналитического исследования, нужны ли практические предложения, какого характера и в какой степени проработки. Если такие предложения у аналитика напрашиваются, но нет уверенности в том, что их от него ждут, можно сказать в заключении, что «при необходимости могут быть выработаны рекомендации по решению рассматриваемой проблемы» или что-то подобное.

Корректность документа. Качества корректного документа (разведывательного, проектного, концептуального):

- практическая направленность;

- минимальный объем;

- ясность формулировок;

- адекватное выражение определенности, вероятности,

- возможности исследуемых сущностей;

- корректное выражение достоверности и точности имеющихся данных;

- проверенность фактов;

- обоснованность выводов;

- зрелость мнений;

- своевременность и уместность, соответствие целям.

Ясность формулировок достигается, прежде всего, использованием распространенных однозначно понимаемых терминов. Надо избегать редких слов, особенно если они имеют более употребительные синонимы. Факты сами по себе малополезны, если не дополняются обобщениями, оценками, практическими выводами.

Зрелое мнение – существующее уже в течение некоторого времени, выдержавшее критику и влияния, освобожденное от явно слабых мест, обросшее аргументами.

Определенность – степень четкости и устойчивости некоторого качества. Если точность – характеристика отражения некоторого качества, то определенность – характеристика самого качества. К примеру, если утверждается: «некто X идентифицирует себя по преимуществу как национал-социалиста, но иногда – как коммуниста», и так оно и есть, то имеет место малая определенность самоидентификации и высокая точность отражения ее наблюдателем.

Вероятность – характеристика повторяющихся событий: среднее количество событий, приходящихся на единицу времени.

Возможность – характеристика неповторяющихся событий.

Точность – относительная или абсолютная величина возможной ошибки в представлении некоторой количественной характеристики.

Достоверность – степень соответствия сведений действительному состоянию отражаемых ими сущностей. Достоверные сведения могут быть неточными, точные – недостоверными. К примеру, если субъект X будет в месте S в день D, то сообщение «X будет в S в день D+3» является точным, но недостоверным, а сообщение «X будет в S в один из дней в промежутке D–2..D+2» является достоверным, но неточным.

Однако о многих важных предметах можно выражаться гладко, эрудированно, остроумно, эффектно, но не по существу.

Отношение разработчика документа к собственному продукту может значительно поменяться в течение короткого времени всего лишь из-за того, что пройдёт творческое возбуждение, препятствующее выработке адекватной оценки. С. М. Штеменко в связи с этим эффектом пишет следующее: «Если (...) позволяет время, не следует докладывать документ тотчас же, как он написан. Надо отложить его на несколько часов, а лучше – до следующего дня, если он не так срочен. В прочитанном, как говорится, на свежую голову документе вы почти обязательно сделаете поправки, часто очень существенные, а иногда (были и такие случаи) документ приходится переделывать».

Представление материалов. Ценное разведывательное сообщение может не произвести само по себе нужного эффекта, если не принять особых мер. Чтобы обеспечить эффект, надо: дождаться подходящей ситуации (или создать ее); соединить документ с другими – создающими нужное настроение; переформулировать сообщение так, чтобы деятель, которому оно адресовано, разглядел в нем свой личный интерес; и т. д.

Если случается, что какое-то ранее сделанное предположение оказалось правильным, об этом надо обязательно при случае упомянуть. Из документов, готовившихся Райнхардом Геленом в 1942 г.: «Противник, **как мы ожидали**, перешел в наступление

против этой армии на широком фронте...». «Картина еще полностью не ясна, но уже можно сказать: **как и предполагалось ранее**, наметились направления двух главных ударов...». «Развитие обстановки... **подтверждает сделанную нами ранее оценку** противника, как по целям, так и по использованию сил и средств...».

В аналитических материалах иногда бывает выгодно представить собственное мнение автора как чужое – сослаться на «некоторых экспертов» или на «некоторые источники». Этот способ используется, если возникает необходимость высказать что-то очень неприятное для адресата. Случается, что разведывательная служба даже идет на подлог: публикует за границей некоторые материалы через подставное лицо, а позже на них ссылается.

Претензии заказчика аналитического документа к содержанию этого документа могут быть следующие:

1. Несоответствие заданию.

2. Поверхностность суждений, демагогичность.

3. Неполный охват темы, отсутствие существенных деталей.

4. Отсутствие новизны: повторение других источников или ранее представленных материалов.

5. Слабость обобщений и рекомендаций.

6. Сырость материала: недоработанный стиль, явные ошибки.

Чтобы сократить количество несправедливых претензий, надо получать всякое задание в письменном виде, в развернутой формулировке. До начала исполнения задания следует оговаривать свои возможности и предполагаемое качество будущего документа. Поскольку в отношениях с руководством все это часто оказывается нереализуемо, то более или менее значительное недовольство заказчика будет иметь место почти всегда. Если у заказчика не ладятся дела, он склонен искать причину не в себе, а в других людях, и в качестве виноватых могут выбираться, среди прочих, и аналитики.

Если заказчик аналитического документа, получив его через некоторое время, заявляет, что надеялся увидеть материал на несколько иную тему или представленный с несколько иной точки зрения, то это нормально, поскольку перегруженные интеллектуальной работой люди склонны забывать детали устно раздаваемых ими заданий, а также незаметно для себя менять свои мнения.

Чтобы избежать несправедливых обвинений, аналитическая служба должна при всякой возможности обращать внимание потребителей разрабатываемых ею документов на то, что довольно частые ошибки и недоработки в ее «продукции» неизбежны – в силу самого характера аналитической деятельности.

Глава 5. Психологическая безопасность аналитической работы

Высокая напряженность и специфика труда специалистов в области аналитической работы (АР) требует специальных мер и приемов, нацеленных на обеспечение их личной информационно-психологической безопасности (ИПБ). Однако, поскольку в большинстве случаев эти люди, обладающие высочайшей квалификацией в своей предметной области, не проходили специальной подготовки, а приемы интеллектуальной деятельности изучали самостоятельно и бессистемно, постольку в вопросах защиты от разнообразных угроз, проявленных в информационно-психологической сфере, они оказываются фактически безграмотными.

Состояние безопасности можно рассматривать как результат или готовность субъекта к адекватной реакции на существующие или потенциальные угрозы, исходящие от внешней среды. Любые реакции по обеспечению безопасности осуществляются всегда в целях сохранения целостности системы и поддержания устойчивости ее состояния в определенном коридоре жизненных проявлений. Обеспечение безопасности предполагает, прежде всего, наличие у субъекта знаний об имеющихся и возможных угрозах, а также о методах реагирования на них. Прежде, чем говорить об угрозах информационно-психологического характера, которым подвергается аналитик при осуществлении своей профессиональной деятельности, необходимо выделить объект, который подвергается их воздействию. Несомненно, что в данном случае этим объектом является сознание аналитика.

Рассмотрим сознание аналитика как целостную систему, совершающую аналитические операции над разрозненными фрагментами разнокачественной и разноуровневой информации.

Прежде всего, отметим, что любая аналитическая работа предполагает наличие цели, которую можно определить как желаемый результат совершаемого анализа (например: осуществление прогнозирования поведения объекта анализа, выявления тенденций, диагностики состояния объекта в реальном времени и пр.). Однако, в большинстве случаев, имеет смысл апеллировать к цели более высокого иерархического уровня – цели деятельности, в интересах информационного обеспечения которой проводится исследование.

Для достижения поставленной цели аналитику приходится совершать ряд мыслительных операций, в ходе которых первичная информация и модельные миры аналитика претерпевают специфические трансформации, причем различные операции требуют переключения сознания в соответствующие режимы и состояния. Отметим также, что сознание каждого аналитика при этом отличается от сознания другого, как структурными, так и функциональными особенностями, зависящими как от устройства мыслительного аппарата, определяющего логику оперирования информацией, так и от различий в «наполнении» модельных миров, сформировавшихся в сознании аналитика. Эти особенности, вызванные различиями в социальном опыте, образовании и воспитании, которыми в основном и определяется специфика подходов к работе с информацией.

Сознание любого аналитика это, прежде всего – человеческое сознание, а не «сверх-разум», обладающий свойствами «Универсума» и идеальным «аппаратом» обработки

информации. Целостность человеческого сознания (в смысле неизменности его содержания) вообще представляется проблематичной, так как сознание является открытой системой, с помощью которой человек осуществляет процесс познания, а значит – постоянно подвергает данную систему воздействиям внешней среды и изменениям.

Для работы с различными семантическими и семиотическими системами сознанию аналитика требуется включение всех его ресурсов, грамотное управление которыми можно осуществить только при согласованной работе левого и правого полушария, а также – при задействовании всей системы нейронных цепей, участвующих в процессе ассоциативного, сравнительного или обобщающего мышления. Это возможно при высокой степени упорядочения работы головного мозга и устойчивости режима сознательного распределения внимания на совершаемых операциях, причем, заметим - при обязательном и постоянном (на уровне автоматизма) сохранении вектора целеполагания.

Соответственно, система мер по обеспечению безопасности аналитической работы, должна непременно включать в себя меры, направленные на решение задач сознательного (по уровню) и одновременно – автоматизированного (по способу) управления своим сознанием как информационной системой. В ходе АР эта информационная система через подвергаемые анализу информационные продукты взаимодействует с другими информационными системами такого рода, которые выступают в качестве целенаправленно функционирующих источников информации (формируют т.н. «поле анализа»). Иными словами – перед аналитиком всегда стоит задача управления процессом взаимодействия (отношениями) сложных информационных систем.

Объекты внешней среды, с которыми происходит взаимодействие, могут быть как материальными, так и абстрактными. Аналитик, как правило, взаимодействует не с самим объектом непосредственно, а с представлениями о нем, с его информационными «аналогами» (являющимися «продуктом» человеческого же сознания). В процессе взаимодействия, соответственно, можно прогнозировать различные варианты его результатов: от полного разрушения одной из систем – до совершенствования (повышения степени упорядоченности и уровня сложности) обоих. Процесс взаимодействия, соответственно, как и процесс совершения мыслительных операций, происходит по определенным законам и алгоритмам, а значит, может быть переведен аналитиком на уровень сознательного контроля и управления.

Рассмотрим 4 типа взаимодействия систем, для которого можно заранее спрогнозировать результат (причем отметим, что непосредственное взаимодействие возможно только для систем с одинаковым иерархическим уровнем):

1. По «соответствию» – для систем со сходными спектральными характеристиками. Результат – изменение (рост) количественных характеристик (например – массы) совокупной системы.

2. По «дополнительности» – для систем с различными спектрами. Результат – изменение (усложнение) качественных характеристик.

3. «0-транспортировка» – для открытых систем. При взаимодействии происходит разрушение исходных систем по одной из наименее устойчивых компонент. Результат

– полное разрушение одной из исходных систем с последующим многовариантным будущим (частичная деформация, реструктуризация, полный распад и т.п.).

4. «Иерархическое» взаимодействие – для самодостаточных, замкнутых систем. Результат – возникновение более сложных, многоуровневых образований по типу «монополия», «империя» и пр.

Трактуя данные типы взаимодействия на языке аналитической практики, можно отождествить их с 4-мя основными типами аналитических операций, совершаемых над информационным объектом с целью получения желаемого результата:

1. По «соответствию» – Композиция;

2. По «дополнительности» – Специализация;

3. «0-транспортировка» – Декомпозиция;

4. «Иерархическое» взаимодействие – Систематизация;

Каждая из данных операций осуществляется сознанием субъекта по определенному алгоритму, согласно которому мыслительная операция рефлексия представляет собой циклический рефлексивный процесс, образованный повторяющейся пятистадийной последовательностью:

1. Стадия саморефлексии.

2. Стадия актуализации объекта.

3. Стадия атрибуции отношений.

4. Стадия формирования целей.

5. Стадия формирования технологии достижения целей.

Необходимо особо отметить, что, несмотря на общность алгоритма рефлексии, сознание, в зависимости от того, какой тип аналитической операции реализуется между ним и объектом анализа, испытывает качественно отличающиеся состояния.

Очевидно, что, рассматривая специфику совершения мыслительных операций в аналитической деятельности, речь должна идти о специфике подготовки сознания к взаимодействию с теми или иными объектами анализа, в которой можно выделить три наиболее важных направления:

1. Психофизиологическая настройка обоих полушарий мозга, учитывающая специфику режима работы и тип аналитической операции;

2. Психологическая подготовка, учитывающая специфику восприятия и спектр возможных реакций субъекта на объект;

3. Оснащение аналитика соответствующими методами работы с информацией, учитывающее особенности объекта анализа (включая целевые, семантические, семиотические, психологические и прочее).

Суммируя вышесказанное, можно сформулировать три базовых положения:

1. В процессе совершения аналитических операций, субъект (аналитик) пользуется

своим сознанием, которое можно рассматривать как информационную систему;

2. Объекты анализа, какова бы их природа ни была, так же можно рассматривать как информационные системы, наделенные рядом символических признаков, позволяющих сознанию оперировать ими на понятном ему «языке»;

3. В процессе субъектно-объектных отношений происходит взаимодействие двух информационных систем, для которых (зная специфику их содержания или функциональных проявлений) можно рассчитать варианты взаимодействий, а значит – заранее спрогнозировать возможные результаты и последствия воздействия их друг на друга.

Специфика аналитической работы и возможные «угрозы». Рассматривая работу аналитика, как работу его сознания по оперированию информацией различного рода, особенное внимание следует обратить на особенности его сознания вообще и на особенности его психофизического состояния на момент анализа. От этих факторов напрямую зависят специфика восприятия информации и специализация внимания, значительно влияющие как на процесс анализа, так и на его результат.

В принципе, любое сознание «специализировано» под восприятие информации априори: мы все от рождения имеем некий «базис» – собственную ДНК, уже обладающую как сходными, так и отличительными свойствами от ДНК других людей и определяющую «врожденные» особенности типа восприятия, стиля мышления, характера реакций и т.д. Однако, по мере дальнейшего развития, «базисная» модель сознания претерпевает значительные изменения, да и вообще, надо сказать, является самой неустойчивой (постоянно меняющей как свое содержание, так и формы проявлений) системой в человеке.

Весьма важно понимать, какие факторы наиболее способствуют мыслительной активности и эффективности анализа, а какие, наоборот, могут оказать деструктивное влияние на сознание аналитика в процессе работы. Такими факторами являются, например, окружающие условия и режим работы, психофизическое состояние и психологические особенности, методологическая база и уровень методической оснащенности. Параметры мыслительной активности зависят, в том числе, и от того, какую пищу и в каких количествах принимал аналитик до начала работы, с кем и насколько комфортно он общался.

Как видим, достаточно много разнообразных и, часто – неподвластных нам факторов и условий определяют свойства процесса и влияют на качество результатов аналитической работы. Кроме того, существует целый комплекс «угроз» или «опасностей», возникающих при взаимодействии сознания аналитика с большими объемами разнокачественной и разноцелевой информации. Возможность реализации этих угроз определяется как спецификой воздействия того или иного типа информации на сознание, так и особенностями совершаемой над ней операции.

В качестве примера рассмотрим возможные изменения сознания и психологические реакции на них в процессе совершения аналитических операций по вышеуказанным 4-м классам операций:

1. *Композиция*. Данная операция совершается при подборе информации (этап формирования системообразующей среды и отбора нужных для анализа сведений по принципу достаточности и необходимости, а также – под определенные цели и по

заданным критериям). Здесь существует опасность перегрузки всех трех сфер сознания, причем, как количеством, так и качеством воспринимаемой информации (например, у «визуалистов» в процессе восприятия понятийно или эмоционально окрашенной информации будут возникать повышенные нагрузки на образную сферу, особенно, если в информации отсутствует изобразительная компонента).

2. *Специализация.* По сути, данная операция заключается в структуризации и классификации отобранной информации под цели и задачи анализа в условиях многовариантности создаваемых схем и формулируемых решений, что потребует от аналитика удерживания в сознании цели и приоритетов, согласно выбранной стратегии. В этом случае опасность заключается не только в возникновении излишней «напряженности» мозга из-за совершения, в общем-то, насильственных действий над собственной, уже структурированной (в рамках какой-либо логики) системой. Возможен вариант влияния воспринимаемой информации (особенно в случае анализа концепций, теорий, религиозных и пр. систем, содержащих «факты и аргументы» из чужеродной для аналитика онтологической среды) на изменение спектральных особенностей (фильтры) восприятия в целом. Это можно назвать своеобразной «перевербовкой» сознания, когда происходит перестройка собственной системы логики под более сильную (идеологически, эмоциально, методологически – это уже не важно), и в этом случае опасность заключается в «сдвиге» по т.н. «фазе» восприятия, что может вообще сделать аналитика неадекватным и недееспособным как специалиста.

3. *Декомпозиция.* Данная операция представляет собой разделение целого объекта на его составляющие до необходимого уровня детализации. В отличие от творческого процесса генерации, который является психологически более комфортным для человека (поскольку оба полушария работают согласованно и гармонично), операция декомпозиции является сугубо интеллектуальной, что является нагрузкой для левого полушария и требует значительных энергетических затрат. Однако необходимо отметить, что опасность здесь состоит не только в потере неоправданно больших объемов энергии, но и в возможном разрушительном влиянии информации на сознание аналитика в силу того, что продукт декомпозиции уже не является чем-то единым и целостным, а каждая из «подсистем» имеет свои (разноцелевые, а значит – разновекторные) характеристики, поэтому происходит перенапряжение от «рассеивания» сознания при попытке удержать во внимании сразу все разрозненные части. Сознание от состояния устойчивой концентрации и координации может перейти в состояние неустойчивости. Кроме того, разрушительным для него может стать и такой эффект, как преобладание в информационном потоке информации «негативного» свойства (в этом случае разрушению подвергаются не только целевые, но и ценностные характеристики).

4. *Систематизация.* Эта операция заключается, прежде всего, в упорядочении информации по заданной системе критериев и построении качественно новой модели, согласно выбранному эталону. Для ее осуществления необходимо не только умение пользоваться инструментами различных методологических школ (что само по себе является серьезной нагрузкой для сознания) и владение инструментарием высокого уровня сложности, но и особое, системно организованное мышление. Высокий уровень абстракции и уровень сложности анализируемых систем часто требует от аналитика, кроме согласованной работы обоих полушарий и синтетических свойств мышления, способности работать с информацией высокой степени

неопределенности и даже умения входить в т.н. «трансперсональные» (измененные) состояния сознания. Опасность здесь, кроме разрушительных энергетических затрат, заключается, прежде всего, в появлении синдрома «неподготовленного скачка», после которого наступает резкое (на два порядка) снижение уровня сознания, что сопровождается симптомами депрессивного свойства. Это происходит в том случае, если уровень решаемых задач и степень упорядочивания информации выше, чем уровень системной организации сознания аналитика. Наиболее характерными проявлениями подобного феномена являются: чувство «опустошенности», резкое снижение уровня работоспособности (вплоть до временной неспособности «соображать» и вообще - мыслить), разочарование, неудовлетворенность и прочие психические симптомы депрессивного характера. Все это проявляется, как компенсаторная реакция, после того, как аналитик, совершая операцию систематизации, достигает состояния типа «генерации», «озарения», «открытия», затрачивая на это несоразмерные уровню своего сознания усилия.

Данные примеры, естественно не исчерпывают перечень всех опасностей, подстерегающих аналитика в процессе его работы. Сюда можно добавить и такие угрозы информационно-психологического характера, как влияние дезинформации, информации откровенно манипулятивного свойства, а также – специально организованной для целенаправленного деструктивного воздействия на аналитика, но эти вопросы достаточно освещены в работах широкого круга специалистов в области информационно-психологической безопасности.

В данном разделе речь идет о безопасности аналитической работы, а потому особое внимание уделяется другого рода опасностям и угрозам и, прежде всего, опасности разрушения целостности сознания как сложноорганизованной информационной системы, возникающим в процессе совершения аналитических операций. Для обеспечения безопасности сознания аналитика при работе со сложными информационными системами крайне важным представляется освоение специальных психотехнологий, могущих решать столь сложные и разнокачественные проблемы, описанные выше.

Методы. Выход видится в универсальности методов управления сознанием, могущих обеспечить т.н. «автоматизацию» его работы под цели и задачи анализа независимо от характера и свойств анализируемой информации. К числу таковых методов, доказавших свою дееспособность и эффективность в разных сферах, являются методы целевого программирования сознания.

Вопросы грамотного целеполагания и автоматического удержания цели в процессе аналитической работы являются ключевыми с точки зрения не только обеспечения безопасности и сохранения информационного иммунитета, но и с точки зрения эффективности аналитической работы в целом. Причем, отметим, что целеориентированное сознание – залог не только устойчивости информационного, но и психического, а также и физического иммунитета, хотя одного этого качества, безусловно, недостаточно для обеспечения безопасности на высоком уровне.

Вниманию слушателей предлагается краткое описание содержания только одного из методов, используемых в практике подготовки сознания к аналитической работе. Безусловно, всегда наиболее продуктивным является освоение практических психотехник непосредственно на тренингах, но возможно, часть слушателей сможет воспользоваться (при понимании смысла и принципа работы) и приведенным здесь

описанием.

Психографическая методика «Пси-алгоритм» является основой технологии управления сознанием и его целевой ориентации. Эта технология, в отличие от применяющихся в подобных целях других психографических методов, алгоритмизована, что позволяет субъекту рефлексии в процессе зарисовки прочувствованных понятийно заданных фрагментов реальности:

- осуществлять процесс самоактуализации;

- целенаправленно выбирать объект воздействия;

- сосредотачиваться на ключевой проблеме субъектно-объектных отношений;

- настраиваться на поиск механизмов ее решения;

- актуализировать эталон собственного «я» после мысленного акта позитивного воздействия на субъектно-объектные отношения.

С помощью данной технологии решается задача активизации всех трех сфер сознания, что позволяет субъекту воздействовать на основу своей психологической сущности (т.н. «подсознание») и, через изменение себя, опосредованно влиять на восприятие объекта управления, придавать его модели целеопределенный характер (аспектуализировать модель). Методика «Пси-Алгоритм» отражена следующим сценарием (рис. 1).

Рис. 1. Сценарная модель алгоритма

На практике данный алгоритм реализуется посредством решения практических проблемных задач субъекта, отображаемых графически в пространстве пустого квадрата (в последовательности слева направо, при этом следуя принципам т.н. «автоматического письма», после получения чувственных или образных результатов концентрации внимания на понятиях) до ощущения полноты, достаточности изображения. Например, так, как это показано на рис. 2.

Рис. 2. Иллюстрация использования алгоритма

При этом мы имеем графический вариант изображения «Я» – «Я», позволяющий

регистрировать изменения субъекта и объекта в динамике алгоритма и оценить характер изменений (например на основе сравнения гармоничности образа, т.е. условно – приближения к идеалу самопредставлений и самоощущений).

Вышеуказанный алгоритм является частью «матрицы алгоритмизации» (МА), состоящей из 3-х (малая МА) или 9-ти (большая МА) рядов подобных алгоритмов по работе с одним и тем же объектом в различных временных интервалах.

Практика использования данного метода показывает устойчивую закономерность: после осуществления нескольких попыток работы данным инструментом (по отношению к различным объектам), кроме повышения уровня осознанности, субъект, как правило, повышает и эффективность решения аналитических и управленческих задач, а также (работая с психосоматическими состоянии) улучшает свое физическое здоровье.

Методика, по существу, является универсальным инструментом управления сознанием в процессе подготовки его к управлению сложными системами, так как за счет эффекта воздействия на все три сферы сознания в совокупности с активизацией рефлексивных процессов. При этом происходят качественные изменения состояния сознания, оно обретает целевую направленность на решение поставленных задач, а также – «автоматизированный» уровень управления сознанием в процессе их осуществления.

Опыт практического применения данного комплекса психотехник показал значительное повышение эффективности интеллектуальной деятельности при совершении субъектами интеллектуальных операций высокого уровня сложности, чего не обеспечивали иные методики, известные практической психологии. Более того: результаты от применения рассмотренных в работе методик достигаются за значительно меньшие сроки, нежели при применении иных методик, традиционно использовавшихся для решения подобных задач.

Выводы. Особенности аналитической работы, всегда требующей значительных интеллектуальных, психических и физических затрат, накладывают особые требования к уровню развития и степени упорядоченности сознания аналитика еще на стадии его подготовки к аналитической практике.

Программа подготовки аналитика по работе со сложными системами должна включать и высокого уровня методологии (как общесистемные, так и предметные), и достаточно серьезное модельное обеспечение (на уровне теоретических метамоделей), и хорошую школу психологической и физической подготовки (включая и тренинговую практику по управлению сознанием и методы психофизической саморегуляции).

В принципе, любой человек по роду своей деятельности вынужден постоянно осуществлять анализ и принимать управленческие решения. Чаще люди не осознают и даже не чувствуют изменения в своем сознании, происходящие в процессе энергоинформационного обмена между ними и средой, а потому – сдают свое сознание в «аренду» тем, кто владеет различными средствами манипуляции. Для аналитика, стремящегося быть объективным и адекватным решаемым задачам, такой подход и вовсе немыслим.

Серьезное, ответственное отношение к себе и сознательная практика в деле обеспечения информационно-психологической безопасности сознания – залог

дееспособности и успешной практики. А если вспомнить, что происходит это в условиях набирающей обороты информационной «войны» (впрочем, являющейся всего лишь одним, но все же достаточно жестким, проявлением закона эволюции – естественного отбора и селекции человеческой «породы»), то и вовсе – психического и физического выживания.

Заключение

Аналитиками не рождаются, ими становятся в результате упорного труда. Это не расхожая фраза. Все это доказано практикой. В принципе, любой человек с высшим образованием может научиться готовить (писать) аналитические документы, работая в аналитической службе безопасности.

Основными трудностями, с которыми сталкивается начинающий аналитик в повседневной работе, являются обычные пробелы в элементарном школьном и вузовском образовании, и, прежде всего, слабое знание русского и иностранного языка. В силу данных обстоятельств он не может на первых порах грамотно изложить свои мысли и тем более подготовить сто процентный аналитический документ. К этому добавляется отсутствие опыта в логическом мышлении, неразвитость процесса мышления, что приводит к стремлению включить в документ вперемешку, как можно больше имеющегося под рукой информационного материала. Мешает и неумение на первых порах делать выводы из подготовленного документа. Врученный руководству аналитической службой (АС) аналитический материал, со всеми вышеназванными ошибками, естественно, вызовет негативную реакцию. Хорошо, если АС руководит человек воспитанный, прошедший хорошую аналитическую школу. Тогда подключение молодого аналитика к работе может стать настоящей школой обретения мастерства.

В негосударственных структурах безопасности работа по обучению начинающих аналитиков находится в зачаточной стадии, если вообще ведется. Бизнесмену легче взять опытного аналитика и тем самым избавить себя от возможных проблем с молодыми сотрудниками или, что часто делается, заказать анализ своих бизнес – проблем какому-либо информационно – аналитическому агентству (а безопасно ли?).

Вместе с тем, сегодняшняя практика показывает, что криминальный мир, затянувший в свое чрево огромное по объему «серое вещество» и оперативный опыт бывших сотрудников силовых структур, опережает в своем «творческом подходе» к аналитической работе многие спецслужбы и службы безопасности (СБ). Каждая криминальная или террористическая операция тщательно готовится, анализируется все, что возможно. Не раскрываемость огромного количества преступлений становится настоящим бичом для российских спецслужб и негосударственных СБ. Примеры у всех на виду и слуху. Практическая аналитика не панацея от всех напастей, но средство уменьшить их негативные последствия, а иногда и предотвратить самое худшее развитие событий. За аналитикой в структурах безопасности будущее. Приближайте его.

Литература

1. Агапов А.В. Основы федерального информационного права России. – М.: Экономика, 1995.

2. Баяндин Н.И. Технологии безопасности бизнеса: введение в конкурентную разведку. – М. 2002.

3. Демченков В.С. Системный анализ в деятельности предприятий. – М.: 1990.

4. Доронин И.Д. Бизнес-разведка. – 2-е изд., перераб. и доп. – М.: «Ось-89», 2003.

5. Доронин А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия. – Тула.: Гриф и К., 2000.

6. Иванков П.Н. Информационно-аналитическое обеспечение работы службы безопасности предприятия // Системы безопасности связи и телекоммуникаций. 1996. №6.

7. Крысин А.В. Безопасность предпринимательской деятельности. – М.: Финансы и статистика, 1996.

8. Кузнецов И.Н. Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе, ООО Изд. Яуза; М., 2001.

9. Плэтт В. Информационная работа стратегической разведки. – М., 1997.

10. Ронин Р. Своя разведка: Практическое пособие. – Минск: Харвест, 1998.

11. Рейльян Я.Р. Аналитическая основа принятия управленческих решений. – М., «Финансы и статистика», 1989.

12. Ярочкин В., Шевцова Т. Словарь терминов и определений по безопасности и защите информации. – М., 1996.

13. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 1997.

ПРАВОВЫЕ АСПЕКТЫ СИСТЕМЫ БЕЗОПАСНОСТИ

(курс лекций)

Обеспечение безопасной деятельности необходимо для любых предприятий и учреждений, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются для обеспечения их безопасности.

Предназначено для преподавателей и студентов вузов специальностей по направлению безопасности, специалистов по безопасности, руководителей и менеджеров компаний.

СОДЕРЖАНИЕ

Лекция 1. СОСТОЯНИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Вопрос 1. Современные угрозы безопасности предприятия

Вопрос 2. Анализ современного состояния проблемы безопасности

Лекция 2. ПРАВОВЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Вопрос 1. Основные условия успешного решения проблем правового обеспечения деятельности в области безопасности

Вопрос 2. Государственная политика обеспечения безопасности

Вопрос 3. Организационно-правовое обеспечение защиты информации

Лекция 3. ТРЕБОВАНИЯ РУКОВОДЯЩИХ ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НСД

Вопрос 1. Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)

Вопрос 2. Европейские критерии по обеспечению ИБ

Лекция 4. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Вопрос 1. Создание концепции зашиты

Вопрос 2. Правовые основы деятельности Службы безопасности

Вопрос 3. Функции, задачи и особенности деятельности Службы безопасности.

Лекция 5. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Вопрос 1. Правовое регулирование и организация работ по защите информации

Вопрос 2. Руководящие нормативно-технические, методические и организационные документы в области информационной безопасности

Вопрос 3. Организационные мероприятия и процедуры по обеспечению защиты информации в автоматизированных системах

Лекция 6. НАЗНАЧЕНИЕ, СТРУКТУРА, МЕТОДЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вопрос 1. Правовая основа информационной безопасности

Вопрос 2. Система правового регулирования информационной безопасности

Лекция 7. ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ КАК ФИНАНСОВО-ПРАВОВАЯ КАТЕГОРИЯ

Вопрос 1. Правовая основа экономической безопасности

Вопрос 2. Основные угрозы экономической безопасности

Лекция 8. АКМЕОЛОГИЧЕСКИЙ ПОТЕНЦИАЛ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Вопрос 1. Потенциал корпоративной безопасности

Вопрос 2. Условия повышения потенциала корпоративной безопасности

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Практическое занятие 1. КАДРОВАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Практическое занятие 2. МЕТОДИКА ОЦЕНКИ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ ФИРМЫ

Практическое занятие 3. СИСТЕМНЫЙ ПОДХОД В ОБЕСПЕЧЕНИИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Практическое занятие 4. ОБЕСПЕЧЕНИЕ КАДРОВОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ И ОРГАНИЗАЦИЯХ

Практическое занятие 5. ПРАВОВЫЕ АСПЕКТЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В УСЛОВИЯХ КОРПОРАТИВНЫХ КОНФЛИКТОВ

Практическое занятие 6. ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СДЕЛОК

Практическое занятие 7. ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ КУПЛИ-ПРОДАЖИ ПРЕДПРИЯТИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ

ЛЕКЦИЯ 1
СОСТОЯНИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Учебные вопросы:

1. Современные угрозы безопасности предприятия.
2. Анализ современного состояния проблемы безопасности.

Вопрос 1. СОВРЕМЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ПРЕПРИЯТИЯ

Обеспечение безопасной деятельности необходимо для любых предприятий и учреждений, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются для обеспечения их безопасности.

Поэтому, анализируя современное состояние проблемы защиты, необходимо выбрать такой объект, в котором "аккумулировались" бы все основные особенности защиты. Одним из таких объектов является банковская система. Банк является наиболее разветвленным, постиндустриальным субъектом экономики, концентрирующим в себе огромный экономический потенциал и, естественно, привлекающий внимание злоумышленников (ЗЛ).

Прежде чем приступить к анализу современного состояния проблемы безопасности, необходимо определить, что подлежит защите и каким основным принципом следует пользоваться. По сложившейся международной практике безопасности объектами защиты с учетом их приоритетов являются:

1) личность;

2) информация;

3) материальные ценности.

Если приоритет сохранения безопасности личности является естественным, то приоритет информации над материальными ценностями требует более подробного рассмотрения. Это касается не только информации, составляющей государственную или коммерческую тайну, но и открытой информации.

Рыночные отношения с их неотъемлемой частью - конкуренцией обязательно требуют противодействия внешним и внутренним угрозам. Объекты защиты в большей или меньшей степени, в зависимости от целей ЗЛ и от конкретных условий, могут подвергаться различным нападениям, угрозам или находиться в ситуации, в которой они по объективным причинам подвергаются опасности.

Понятие "безопасная деятельность" любого предприятия или организации включает в себя:

1. Физическую безопасность, под которой понимается обеспечение защиты от посягательств на жизнь персонала.

2. Экономическую безопасность.

3. Информационную безопасность.

4. Материальную безопасность, т.е. сохранение материальных ценностей от всякого рода посягательств, начиная от их краж и заканчивая угрозами пожара и других стихийных бедствий.

1.1. Угрозы экономической безопасности

Угрозы экономической безопасности деятельности банка могут быть самыми различными, но мы выделим только основные угрозы, которые входят в компетенцию СБ.

К данному виду угроз в первую очередь относятся угрозы от:

1) отдельных сотрудников банка;

2) криминальных российских структур;

3) криминальных зарубежных структур;

4) международных криминальных структур.

Несмотря на очевидность данных угроз, проиллюстрируем их на наиболее ярких конкретных примерах.

В феврале 1995 года обанкротился крупный английский банк "Беринге". Это произошло потому, что работник банка Ник Лисон проводил незаконные сделки через счет, который был открыт еще в 1992 году. Убытки в 830 млн. фунтов стерлингов накапливались в течение долгого времени. Ни руководство банка, ни аудиторы, ни контролеры не выявили за это время никаких нарушений. Одной из причин явилось то, что Ник Лисон отвечал как за торговые операции, так и учетную документацию по операционной деятельности, а руководство банка не осуществляло должный контроль за раздельным ведением клиентских и собственных счетов брокеров.

В 1994 году пресечена деятельность преступной группы, состоящей из работников РКЦ ГУ ЦБ по Новосибирской области, Сибирского филиала Инкомбанка и представителей фиктивной коммерческой фирмы Группа путем перечисления денег по фальшивым платежным документам на счет этой фирмы похитила почти 1,4 миллиарда рублей.

В тяжелых условиях становления рынка положение банков усугубляется мощным и все возрастающим давлением со стороны криминального мира. Ни для кого не является секретом, что многие коммерческие фирмы прямо или косвенно связаны с

мафиозными структурами или существуют за счет их средств.

Происходит постепенное сращивание российского и зарубежного преступного мира.

В условиях политической и экономической нестабильности и при наличии различного рода угроз (от неплатежеспособности до мошенничества) является естественным объединение усилий коммерческих структур для сохранения их экономической безопасности. Примером этому является соглашение между банками "Империал", "Столичный" и другими, направленное на сотрудничество и деятельность по предотвращению недобросовестной конкуренции, что, несомненно, повысит степень их экономической защищенности.

Учитывая высокий уровень латентности экономических преступлений, приведенные цифры лишь отчасти отражают процесс последовательного роста темпов криминализации экономики, сопровождающийся расширением масштабов проникновения в нее организованных преступных группировок, все более тесного смыкания с работниками органов государственного управления, в том числе на самом высоком уровне.

Прогнозы на ближайшее будущее предполагают появление новых и усиление общественно опасных форм преступной деятельности в сфере кредитно-денежных отношений (махинации с векселями, кредитными карточками, незаконная эмиссия ценных бумаг и т.п.).

В общем виде можно сформулировать основные угрозы экономической безопасности банка:

- плохая адаптированность существующей банковской системы к условиям рынка;

- общая неплатежеспособность;

- невозврат ссуд;

- лжепредпринимательство;

- мошенничество;

- подрыв доверия.

Наличие данных угроз обусловлено следующими видами риска:

1) риск утечки, уничтожения или модификации банковской информации;

2) риск отсутствия у руководства банка объективной информации о внутренней и внешней среде;

3) риск распространения конкурентами во внешней среде необъективной или опасной для банка информации.

Таким образом, обеспечение коммерческой деятельности банка или любой фирмы включает в себя не только защиту информации, но и сбор, классификацию, анализ, оценку и выдачу прогнозов для успешной коммерческой деятельности. Говоря другими словами, чем выше информационное обеспечение банка, тем менее возможны угрозы его экономической деятельности.

1.2. Угрозы физической безопасности

В настоящее время участились случаи нападения на банкиров и служащих банка. Как правило, это прежде всего руководители коммерческих банков и фирм, которые в течение длительного времени (например, для запугивания, склонения к сотрудничеству и т. п.) или, наоборот, короткого промежутка времени (ограбление или убийство) являются объектом нападения со стороны преступников. Примеров тому достаточно.

Профессор А.В. Крысин в статье "Деятельность коммерческих банков (фирм) в условиях роста террористической угрозы" (см.: Частный сыск, охрана, безопасность, 1994, № 1) отмечает следующие методы воздействия на сотрудников коммерческих объектов:

- похищения и угрозы похищения главы и членов семьи;

- убийства, сопровождаемые насилием, издевательствами и пытками;

- психологический террор, угрозы, шантаж, вымогательство;

- публикация дезинформационных материалов о текущей деятельности некоторых коммерческих организаций, которые прямо направлены на их дискредитацию и компрометацию отдельных сотрудников;

- инспирация официальных заявлений от имени некоторых органов массовой информации и представителей исполнителей массовой власти, в которых подытоживается деловая репутация и наносится моральный и материальный ущерб отдельным коммерческим банкам, фирмам.

При этом выделяются следующие основные методы и приемы диверсионно-террористической деятельности:

- взрывы;

- обстрелы из автоматического оружия различных калибров и сигнальных ракетниц;

- минирования, в том числе с применением дистанционного управления;

- поджоги, броски канистр и иных емкостей с легко воспламеняющимися жидкостями и смесями;

- нападения, вторжения, захваты, пикетирования, блокирования;

- акты вандализма, повреждение входных дверей, решеток, ограждений, витрин, витражей, мебели, а также транспортных личных и служебных средств.

Цель подобных акций:

- откровенный террор в отношении коммерческих структур;

- нанесение им серьезного материального и морального ущерба, который в ряде случаев составляет десятки тысяч долларов США;

- срыв на длительное время, порой до нескольких месяцев, нормального функционирования коммерческого предприятия;

- вымогательство значительных сумм денег или каких-либо льгот (кредиты, отсрочки платежей и т.п.) перед лицом террористической угрозы.

Одной из реальных мер обеспечения физической безопасности является доведение до служащих защищаемого объекта, которым может угрожать опасность, обязательных правил поведения с учетом сложившейся обстановки, характера угрозы, возможного времени и места ее реализации и мероприятий, обеспечивающих их безопасность. Однако способы реализации угроз могут быть самые различные. Поэтому данные указания и советы могут носить лишь общий характер, поскольку преступники находят все новые и новые пути для достижения своих целей.

Резюмируя, можно сказать, что в настоящее время ни один человек не может чувствовать себя в безопасности. Различного рода преступления не получили бы такого широкого распространения, если бы банкиры уделяли должное внимание организации работы СБ. Обеспечение личной безопасности - напряженная работа. Банкир может попасть в "зону риска", и применение определенных методов охраны требует определенной системы поведения не только от охранников, но и от объекта охраны. Это обусловлено тем, что преступники предварительно собирают информацию о жертве, изучают "слабые места" и широко ими пользуются. Без необходимой информации об объекте нападения значительно увеличивается степень риска для преступников. Поэтому необходимо скрывать любую информацию, которую преступник может использовать при подготовке или совершении преступления. Важно отметить, что убийства, как правило, остаются нераскрытыми, что наводит на естественную мысль о хорошей организации и подготовке преступников.

1.3. Угрозы информационной безопасности

Как считают западные специалисты, утечка 20% коммерческой информации в шестидесяти случаях из ста приводит к банкротству фирмы. Ни одна даже преуспевающая фирма США не просуществует более трех суток, если ее информация, составляющая коммерческую тайну, станет известной. Таким образом, экономическая и информационная безопасность банка или фирмы тесно взаимосвязаны.

Уменьшение угрозы экономической деятельности банка предусматривает получение информации о конкурентах. Поэтому, вполне естественно, уменьшение данной угрозы для одних банков влечет за собой увеличение угрозы экономической деятельности для других банков. Это стало возможным из-за наличия промышленного и, в частности, банковского шпионажа.

Ущерб от деятельности конкурентов, использующих методы шпионажа, составляет в мире до 30% всего ущерба, а это - миллиарды долларов. Точную цифру убытков указать нельзя по следующей причине: ни ЗЛ, ни пострадавшие не стремятся предать гласности совершенные действия. Первые, боясь ответственности за содеянное, а вторые - из-за боязни потерять имидж. Этим объясняется высокий уровень латентности правонарушений и отсутствие о них информации в открытой печати. Поэтому до читателей доходит менее 1% от всех случаев нарушений, которые обычно имеют уголовный характер и которые скрыть нельзя.

Банковский шпионаж использует самые разнообразные приемы: "классические" методы шпионажа (шантаж, подкуп и т.п.), методы промышленного шпионажа, несанкционированное использование средств вычислительной техники, аналитические методы. Возможность использования указанных методов появилась потому, что банковская информация имеет различные формы представления (документ, человеческая речь, машинный носитель и т.п.) и, следовательно, различные способы ее передачи, хранения и обработки. Поэтому спектр угроз информационной безопасности весьма широк.

Промышленный шпионаж достаточно развит в западных странах. Сотни фирм специализируются на изготовлении средств технической разведки и на проведении мероприятий по промышленному шпионажу. В последнее время он получил распространение и в нашей стране. Масштабы промышленного шпионажа можно оценить хотя бы по следующему факту - на проходившей в 1995 году выставке-продаже зарубежных и отечественных средств технической разведки было продано 70 тыс. единиц средств добывания информации и только единицы их поиска и борьбы с ними. А всего на выставке было представлено более 2000 видов различных устройств. В настоящее время около 200 российских и зарубежных фирм торгуют на территории России и стран СНГ средствами промышленного шпионажа и контршпионажа. Рост конкуренции стимулирует спрос на оборудование промышленного шпионажа.

За последнее время накопилось немало примеров, когда потери коммерческих структур от утечки информации за счет промышленного шпионажа превосходили размеры прямых потерь от краж или разбойных нападений. Нельзя недооценивать возможности промышленного шпионажа и ущерб, который он может принести банку или фирме. Страшно представить, какой ущерб может принести банку закладное устройство стоимостью всего $10 в случае его удачного размещения. Примеров тому достаточно - читатель сам знает о них, а исходя из ранее сказанного они (примеры) не приводятся.

Используют средства и методы промышленного шпионажа, как правило, либо недобросовестные конкуренты, либо мафиозные структуры. Причем последние, в отличие от примитивной уголовщины, имеют свою собственную разведку и контрразведку, а на их техническое оснащение новейшими и дорогостоящими средствами не жалеют денег.

Противодействие получению информации с помощью технических средств разведки (ПДТР) достаточно сложно и по силам только специалистам, имеющим практический опыт. Это объясняется следующими основными причинами:

- в общем случае неизвестно, кто, когда, в каком месте и каким образом попытается получить информацию;

- приобретение средств промышленного шпионажа не вызывает затруднений;

- правовая регламентация использования средств промышленного шпионажа несовершенна. С помощью средств промышленного шпионажа не только различными способами подслушивают или подсматривают за действиями конкурентов, но и получают информацию, непосредственно обрабатываемую в средствах вычислительной техники. Это уже стало повседневным явлением (например, съем информации с дисплеев или линий связи ЭВМ). Однако наибольшую опасность здесь

составляет непосредственное использование ЗЛ средств вычислительной техники, что породило новый вид преступлений - компьютерные преступления, т. е. несанкционированный доступ к информации (НСД), обрабатываемый в ЭВМ.

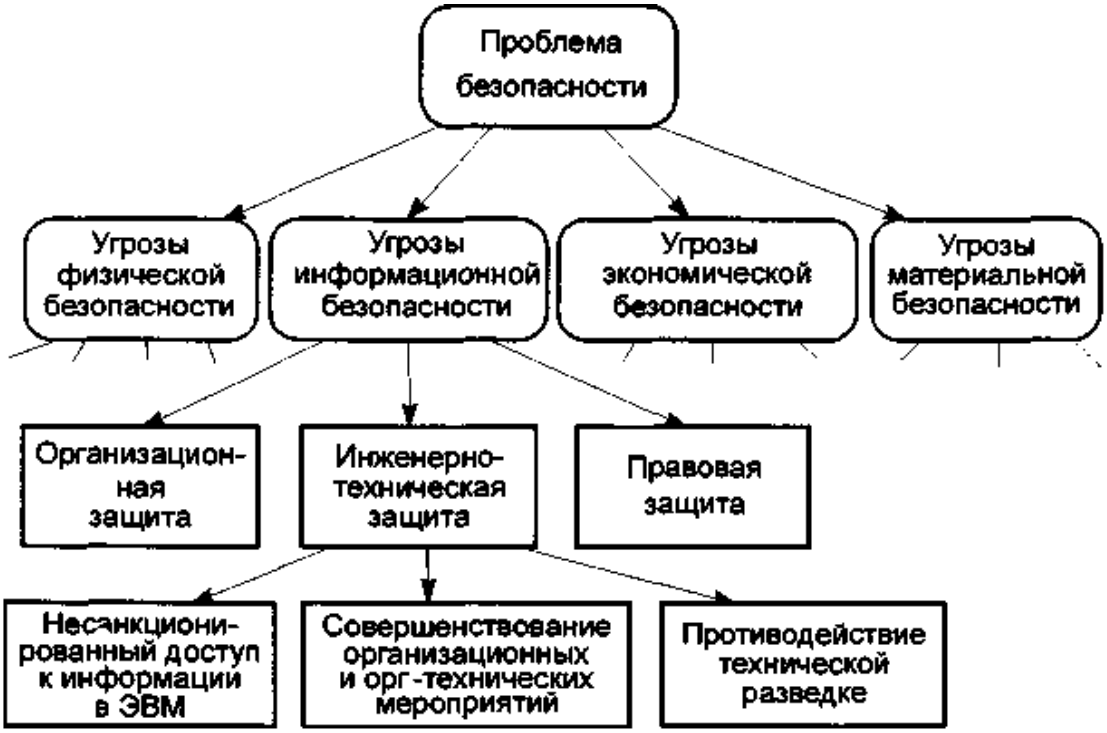


Рис 1. Проблемы и направления обеспечения безопасности

По мнению зарубежных экспертов, ущерб, нанесенный банкам США за счет несанкционированного использования вычислительных сетей путем введения и "навязывания" ложной информации из Москвы и Санкт-Петербурга российскими мафиозными структурами, только за I квартал 2005 года составил $300 млн.

Контрольные проверки, проведенные несколько лет назад по просьбе ряда банков Москвы специалистами Гостехкомиссии России и Российского центра "Безопасность", показали, что при использовании вычислительных сетей относительно просто войти в базы данных, считать и изменять их содержимое, подделывать переводы и т.п.

Приведенные примеры показывают, что использование средств вычислительной техники раскрывает новую область для промышленного шпионажа. При этом ЗЛ могут не только получить доступ к открытой информации, но и к информации, содержащей коммерческую и государственную тайну. Если студент-хакер может войти в сеть НАТО, как это было совсем недавно, и получить секретную ключевую информацию, то в коммерческую вычислительную систему может войти и программист-профессионал, оставшийся без работы и нанятый конкурентами или мафиозными структурами. А если можно войти в вычислительную систему, то можно не только получить информацию, но и всю ее уничтожить, модифицировать или манипулировать. В силу этого банк или фирма потерпят убытки или станут на грани финансового краха из-за невозможности выполнения своих функций.

В настоящее время в зарубежных странах появились информационные брокеры, которые с помощью хакеров взламывают СЗИ, получают информацию, а затем ее

продают. Покупателями могут быть как конкуренты пострадавшей фирмы, так и сама пострадавшая фирма.

Понятие "компьютерная преступность" включает в себя несколько позиций. В него входят несанкционированное проникновение в сети, хищение времени ЭВМ и изменение информации ("логической бомбы", вирусы и т.д.), также противоправные действия с использованием компьютерной техники:

- различные виды мошенничества, связанные с неправомерным использованием пользовательских терминалов, осуществление международных денежных переводов (вследствие чего фирмы несут убытки, исчисляемые сотнями тысяч долларов), незаконное изготовление и подделка электронных средств платежа и их использование для хищения наличных средств из банкоматов;

- несанкционированное тиражирование компьютерных продуктов и т.д. (компьютерное пиратство);

- компьютерный саботаж;

- распространение по международным информационным сетям материалов порнографического содержания, экономический шпионаж и пр.

Более подробно о преступлениях в сфере компьютерной информации, согласно российскому законодательству, см.: Комментарий к уголовному кодексу РФ. М., Юрист, 1997 г., ст. ст. 272-274.

В части компьютерных преступлений Россия не отстает от зарубежных стран. В 2001 году начальник отдела автоматизации неторговых операций вычислительного центра Внешэкономбанка совершил кражу на сумму $125000 США. Из материалов уголовного дела, возбужденного по факту кражи, следует, что хищение валютных средств было выполнено с помощью несанкционированного изменения не только программного обеспечения, но и манипуляций с данными по счетам клиентов банка. Имея возможность доступа к ЭВМ по роду своих служебных обязанностей, начальник отдела автоматизации незаконным путем создал излишки валютных средств (резерв) на некоторых счетах, которые впоследствии, также незаконным путем, перераспределялись на другие счета, в том числе открытые по поддельным документам. Информация на машинных носителях ЭВМ о движении средств по этим счетам впоследствии корректировалась с целью пополнения на них запасов валютных средств. Компьютерная система банка в данном случае служила инструментом, аналогичным по функциональному назначению средствам, обычно используемым для подделки документов.

Необходимость совершенствования защиты банковской информации и телекоммуникационных систем подтверждается растущим числом фактов незаконного обладания финансовой информацией.

ЦБ России в 2006 году выявил подделанных финансовых документов на сумму около 450 млн. рублей. Это стало возможным благодаря использованию новой СЗИ компьютерной и телекоммуникационной сети. Точной цифры потерь российских коммерческих банков, обусловленных недостаточностью внимания к безопасности информации, не знает никто. Однако есть все основания предполагать, что они большие.

Противодействовать компьютерной преступности сложно, что главным образом объясняется:

- новизной и сложностью проблемы;

- сложностью своевременного выявления компьютерного преступления и идентификации ЗЛ;

- возможностью выполнения преступлений с использованием средств удаленного доступа, т.е. ЗЛ на месте преступления нет;

- трудностями сбора и юридического оформления доказательств компьютерного преступления.

Учитывая большой ущерб от компьютерных преступлений, в настоящее время стали широко внедряться криптографические средства защиты информации, которые обладают гарантированной стойкостью защиты. Однако и они не являются панацеей для защиты информации, т.к. защищают только часть спектра, а не весь спектр угроз информационной безопасности.

Промышленный шпионаж широко использует опыт военной разведки, из которого известно, что 90% информации о противнике можно получить косвенным путем. При этом источниками информации о конкурентах являются:

- информация, содержащаяся в средствах массовой информации, целенаправленная на исследуемый объект;

- сведения, распространяемые непосредственно конкурентом, его служащими или клиентами;

- финансовые отчеты, проспекты, брошюры, рекламные издания, запросы и т.д.;

- переговоры со служащими и клиентами конкурента;

- непосредственное наблюдение за объектами конкурентов.

Сбор подчас многочисленных и отдельно взятых незначительных сведений позволяет получить практические прогнозы и нередко - достоверные выводы об экономическом состоянии конкурента для принятия тактических и стратегических решений в целях обеспечения собственной экономической безопасности. Например, регулярные наблюдения за автомашинами, подъезжающими к зданию банка-конкурента, позволяют выявить его клиентов, их взаимоотношения с банком, деловую активность банка и т.д.

Знания о покупках программного обеспечения для средств вычислительной техники позволяют направить исследования с целью выявления недокументированных функций и последующее их использование для нарушения работы средств вычислительной техники.

Незначительная на первый взгляд информация при значительном объеме обеспечивает переход количества в качество при ее обобщении и аналитической обработке.

1.4. Угрозы материальной безопасности

В последние годы участились нападения на банки и их филиалы.

Особую проблему составляет обеспечение безопасности при перевозке денежных средств. Один из фактов: в Екатеринбурге совершено нападение - пропали сотрудники УБРР и один миллиард рублей. Этот пример показывает высочайшую подготовку и прекрасное информирование преступников о деятельности СБ.

Защита банков и инкассаторов от ограбления в значительной степени зависит от их технической оснащенности. Если защита банков традиционна, то техническое оснащение инкассаторов требует специальных автомашин-сейфов, закрывающихся кодовыми замками, которые невозможно открыть в пути. Поэтому деньги можно похитить только вместе с машиной.

Следует особо отметить, что нападения на инкассаторов в большинстве случаев совершаются при участии или наводке сотрудника ограбленной коммерческой структуры. Таким образом, СБ должна вести работу с персоналом для выявления их сомнительных связей и т.п. Подобная деятельность носит название "обеспечение внутренней безопасности".

Годы труда могут пойти прахом за считанные секунды. Выживание или крах коммерческой организации часто зависит от степени готовности СБ к различного рода неожиданностям. Приведем лишь три примера.

В 1989 г. небольшой пожар в помещении страховой компании Penn Mutual уничтожил информацию в компьютерном зале компании, т.к. 15 млн. литров воды залили его.

Аналогичный пример пожара в 1995 г. имел место в Москве в Промстройбанке, где погиб один человек и был нанесен ущерб в размере 10 млн. долларов. По словам председателя правления, банковская информация не пострадала, однако он признал, что банк не готов к подобным чрезвычайным последствиям (МП) с точки зрения ее защиты.

В мае 1996 г. пожар во французском банке "Кредит лионз" нанес ущерб в 350 млн. долларов.

Следует обратить внимание на высокий процент ущерба от пожаров, связанных с поджогами. Так, в США поджог - самый быстрорастущий вид преступления, и каждый второй пожар вызван поджогом. Как показали исследования, такая статистика типична для многих стран и не зависит от типа политического или государственного устройства.

Журнал "Survivel" сообщает, что 150 из 350 деловых организаций, функционировавших в Международном торговом центре до взрыва в 1993 г., спустя год прекратили свое существование.

Бедствия, такие как пожары, взрывы, ураганы, наводнения, землетрясения, нарушения электропитания и т.п. трудно предсказуемы, хотя и относительно редкие, но могут привести к значительным убыткам. Но восстановление деловой активности после подобных ситуаций должны быть четко спланированы СБ. Централизованное

управление процессом восстановления важно для поддержания деятельности организации, ее способности предоставить заказчикам хотя бы минимум услуг, иначе коммерческий крах неизбежен.

Вопрос 2. АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ПРОБЛЕМЫ БЕЗОПАСНОСТИ

Обобщая и анализируя вышеприведенные примеры угроз безопасности, можно выделить три основные составляющие проблемы безопасности:

1. Правовая защита.

2. Организационная защита.

3. Инженерно-техническая защита

Раскроем содержание каждого направления. Смысл обеспечения правовой защиты ясен из самого названия. Организационная защита включает в себя охрану и режим работы объекта. Под инженерно-технической защитой понимается совокупность инженерных, программных и других средств, направленных на исключение угрозы безопасности.

Вполне естественно, что для каждого вида угроз безопасности должны использоваться различные правовые, организационные и инженерно-технические мероприятия. Это обусловлено различным характером угроз. Целью анализа является рассмотрение возможности СБ предупредить, выявить и "устранить" ЗЛ.

Анализ зафиксированных фактов и уголовных дел, связанных со всеми видами безопасности, свидетельствует о стремительном росте правонарушений. Убийства, мошенничество, промышленный шпионаж и т.п. уже превратились в реальный фон деятельности как государственных, так и коммерческих структур. Положение можно охарактеризовать, как напряженное, что обусловлено:

- крайне тяжелой экономической обстановкой в стране, расслоением общества на "очень богатых" и "очень бедных", падением уровня социальной защиты населения;

- отсутствием должной координации деятельности правоохранительных органов, специальных служб, суда, прокуратуры и негосударственных СБ;

- сложностью учета правонарушений в экономической сфере;

- отсутствием необходимого опыта выявления и пресечения новых видов преступлений в экономике;

- ухудшением криминогенной обстановки.

Учитывая международный характер и масштабы преступлений, их предотвращение и борьба с ними требует активных международных усилий. Даже самое идеальное решение правовых и законодательных вопросов обеспечения безопасности не обеспечит ее сохранения, если не будет работать организационный механизм, претворяющий в жизнь данные положения. В настоящее время такой механизм только зарождается, его развитию препятствует политическая и экономическая

нестабильность.

Анализ возможностей технического обеспечения блокирования угроз безопасности (инженерно-техническая защита) может быть проведен из расчета того, что ЗЛ (конкуренты и мафиозные структуры) и СБ обладают одинаковыми возможностями в оснащении.

Мировой уровень технического состояния противодействия попыткам нарушения безопасности достаточно высок. Однако для практической деятельности необходимо выполнение двух основных условий:

- наличие средств на закупку и эксплуатацию СЗ,

- наличие необходимого уровня подготовки персонала.

При наличии этих основных условий можно противостоять любым попыткам злоумышленных действий, однако в настоящее время главный акцент в деятельности СБ коммерческих структур пока грешит силовым подходом к проблеме безопасности в целом, делая ставку на мускулы охранников, а не на интеллект и техническую оснащенность. Попутно отметим, что имеющийся сейчас силовой подход имеет низкий уровень подготовки, который не соответствует сложившейся криминогенной обстановке и международной практике.

Представляет интерес сравнение объема финансирования СБ стран Западной Европы и России. Первые расходуют от 15 до 25% годовой прибыли. Анализ средств, расходуемых на содержание СБ коммерческими банками России, показывает, что многие из них тратят менее 1% от годовой прибыли. Дальнейшее ухудшение криминогенной ситуации в России неизбежно приведет российских бизнесменов к необходимости тратить на безопасность фирмы или банка столько же, сколько их западные коллеги, если не больше.

Вывод: обеспечение безопасности является одним из базовых факторов, определяющих как саму возможность экономической деятельности, так и ее стратегические направления.

Несовершенство правового законодательства и, как следствие, отсутствие единого отлаженного механизма обеспечения безопасности коммерческой деятельности приводит к тому, что основная тяжесть данной проблемы ложится непосредственно на коммерческие структуры.

Однако в настоящее время появилась тенденция к стабилизации положения в области безопасности коммерческой деятельности.

ЛЕКЦИЯ 2
ПРАВОВЫЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Учебные вопросы:

1. Основные условия успешного решения проблем правового обеспечения деятельности в области безопасности.
2. Государственная политика обеспечения безопасности.
3. Организационно-правовое обеспечение защиты информации.

Вопрос 1. ОСНОВНЫЕ УСЛОВИЯ УСПЕШНОГО РЕШЕНИЯ ПРОБЛЕМ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ БЕЗОПАСНОСТИ

Ряд экспертов в области безопасности, исходя из опыта развития ситуации в последние 30 - 40 лет, пришли к заключению, что в качестве основополагающих предпосылок успеха в решении проблем правового обеспечения деятельности в этой сфере можно выделить следующие три, приведенные ниже.

1. Совершенствование законодательства

В передовых странах с развитыми системами имущественного страхования большинство людей беспечно относится к вопросам охраны своей собственности в силу того, что уверены в получении страхового возмещения в случае кражи имущества. Это обстоятельство существенным образом облегчает задачу для потенциального преступника. С другой стороны, легкость достижения преступной цели толкает многих на неправедный путь.

На вопрос, над которым ломает голову общественность, кто больше виноват: собственник ли, беспечно и легкомысленно оставивший имущество без присмотра, или воришка, соблазнившийся на легкую добычу, в последнее время юристы склонны отвечать теорией о так называемой обоюдной ответственности. Человек слаб и зачастую не в силах устоять перед искушением, за малым прегрешением следует более серьезное, правонарушитель превращается в преступника, в результате криминогенная ситуация в обществе обостряется.

В настоящее время у специалистов-правоведов не вызывает сомнения, что разработка и принятие законодательных норм, предписывающих обязательное для собственника осуществление минимума мер в области обеспечения безопасности любых объектов собственности, способствовало бы сокращению преступных посягательств против собственности.

Понятие тайны, секрета тесно связано с понятием собственности. В рыночной экономике каждый собственник, в том числе и любой хозяйствующий субъект,

обладает естественным правом за свой собственный счет охранять свои имущественные интересы и права (в том числе право на коммерческую тайну), естественно, без ущерба правам и интересам других собственников и общества в целом. Охранять это право - дорогостоящее дело. Обеспечивать безопасность объектов собственности, к примеру, засекречивать информацию "с запасом" объявляя ее коммерческой тайной, просто невыгодно. Коммерческая тайна наряду с рекламой - элемент маркетинга, и никто, кроме самого собственника и управляющего предприятием, отвечающих за получение прибыли и упущенную выгоду, не может определить необходимые объемы информации, требующие защиты, и соответствующие затраты, которые можно себе для этого позволить.

Казалось бы, противоречие неразрешимо? И все же специалисты склоняются к необходимости учитывать универсальный принцип о том, что право вообще и право собственности, в частности, неразрывно связаны и с определенными обязательствами, налагаемыми на их обладателей.

Так, ряд специалистов в нашей стране полагают, что внесение, к примеру, в банковское законодательство положений об обязательности принятия определенного минимума мер безопасности в наиболее уязвимых для преступных имущественных посягательств финансово-кредитных учреждениях, особенно привлекающих средства частных вкладчиков, способствовало бы сокращению преступности в этой сфере бизнеса. Этому способствовало бы и введение обязательного технического аудита систем защиты, без которого было бы нельзя получить лицензию на этот вид деятельности. Более того, корректировка в этом направлении законодательных актов способствовала бы углублению в обществе понимания важности проблемы безопасности вообще.

2. Необходимость регулирования правоотношений в сфере производства систем и средств безопасности

На Западе общественность уже давно склоняется к тому, чтобы в этой сфере было введено государственное регулирование и лицензирование (как это уже имеет место в Израиле и некоторых штатах США). Одним из элементов государственного регулирования должно быть создание необходимой организационно-правовой и научно-технической базы лицензирования и сертификации, специальных аттестационных и сертификационных центров и лабораторий для проведения тестирования, чтобы пользователь мог иметь возможность отличить хорошее от дурного. Несомненно, что внедрение государственного регулирования в этой области является важным шагом на пути обуздания преступности.

3. Совершенствование систем страхования, связанного с обеспечением безопасности

Ввиду резкого роста экономических преступлений в настоящее время (и в нашей стране это особенно) имущественное страхование становится все более рискованным и менее прибыльным. Очевидна взаимосвязь между страхованием имущества от всевозможных рисков, в том числе связанных с преступными посягательствами и положением дел в области производства и внедрения эффективных средств и систем защиты. Беспечный и легкомысленный собственник, оставляющий раскрытыми настежь двери и окна пустующего дома, провоцирующий тем самым преступника на совершение противоправных деяний, вряд ли может рассчитывать в случае совершения кражи на автоматическое страховое возмещение в полном объеме. Иначе

выплата этого возмещения фактически означала бы прямое субсидирование криминального бизнеса. Процесс страхования поэтому сочетается с мерами, побуждающими собственника-страхователя обеспечивать необходимую безопасность своего имущества.

Размеры страховых взносов (премий), сумм возмещений и другие условия договоров имущественного страхования должны напрямую зависеть от эффективности мер безопасности, предпринимаемых страхователем, разумный обязательный минимум которых было бы целесообразно закрепить законодательно. Кроме того, желательно страхуемому собственнику одновременно с выдачей страхового полиса обеспечить возможность получения специальной подготовки и консультаций (плата за которые входила бы в стоимость полиса), относительно выбора в зависимости от существования тех или иных рисков и угроз подходящего оборудования и систем безопасности, а также их последующего внедрения. В ряде стран (США, Канада, Израиль) такого рода механизм уже запущен, что способствует сдерживанию роста преступлений против личности и собственности.

В условиях нынешней российской действительности, когда страховой рынок лишь формируется, главной заботой многих страховых компаний, к сожалению, является выдача страхового полиса и получение премии. О возможных финансовых последствиях заключенного страхового соглашения страховщики задумываются не всегда, да и порой недосуг, так как подвергать серьезной оценке принимаемые на страхование объекты некогда: того и гляди клиента перехватит менее разборчивый страховщик. Такая ситуация продлится недолго, еще несколько крупных убытков и отечественные страховщики также поймут, что выгоднее прибегнуть заблаговременно к услугам квалифицированных экспертов для оценки страхуемого риска, чем страховать объекты, состояние которых, в том числе эффективность систем обеспечения их безопасности, остается для страховой компании тайной за семью печатями.

Вопрос 2. ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Принципы государственной политики

Информация и информационные ресурсы, как продукты общественного производства, являются объектами права собственности и, следовательно, имеют своих собственников и потребителей (пользователей).

Государственная политика обеспечения информационной безопасности основывается на следующих принципах:

- государство обеспечивает контроль за созданием, сохранностью и использованием национальных информационных ресурсов, а также способствует предоставлению гражданам доступа к мировым информационным ресурсам;

- государство обеспечивает право граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

- засекречивание есть исключение из общего права на доступ к информации; рассекречивание информации осуществляется в установленном законом порядке;

- ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируется;

- любое юридическое или физическое лицо, собирающее, накапливающее и обрабатывающее персональные и любые другие конфиденциальные данные, несет ответственность перед законом за их сохранность и использование;

- перечни сведений, могущих быть отнесенными к конфиденциальной информации или, наоборот, не могущие быть отнесены к таковым, опреде-ляются установленным законом порядком;

- интересы собственников, владельцев и распорядителей информаци-онных ресурсов охраняются законом.

Для претворения в жизнь изложенных принципов необходима соответствующая инфраструктура информационной безопасности.

2.2. Деятельность государства по обеспечению информационной безопасности

Характерной особенностью настоящего этапа развития информационной безопасности является переход от ведомственных, в основном технократических подходов, к комплексному государственному. Возглавляет данную работу Совет Безопасности Российской Федерации. Он поднимает вопрос о разработке конституционных законов в сфере информатизации и информационной безопасности.

Для выработки государственной политики и координации организационно-правовой деятельности в данной сфере в соответствии с Законом РФ "О безопасности" в Совете Безопасности Российской Федерации создана Межведомственная комиссия по информационной безопасности.

Межведомственная комиссия формирует общегосударственный механизм выявления угроз и защиты интересов России в информационной сфере. При этом выделяются три основных направления ее деятельности, а именно обеспечение:

- защищенности системы формирования информационных ресурсов;

- необходимого уровня защищенности применяемых технологий передачи и обработки информации;

- конституционных прав и свобод граждан, законных интересов государства и общества в сфере информатизации.

Таблица 1.

Основные отличия информационного права

Правовые понятия	Вещное право	Исключительное право		Информационное право	
Объект	вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права	результаты интеллектуальной деятельности		информация	
Детализация объектов	недвижимые и движимые вещи, плоды, продукция и доходы, животные, деньги, валютные ценности, ценные бумаги	авторское право	интеллектуальная собственность и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.)	необщедоступная конфиденциальная информация: коммерческая тайна, банковская тайна, тайна страхования, тайна связи, иная служебная тайна, персональные данные	личная и семейная тайна
Характер права	публичное	частное	публичное	публичное	частное
Оборотоспособность	могут свободно отчуждаться или переходить от одного лица к другому	неотчуждаемы	ограниченно оборотоспособные	ограниченно оборотоспособные	неотчуждаемая
Субъект правоотношения	дееспособные физические и юридические лица	любые физические и юридические лица		любое лицо, обладающее сведениями или профессионально занимающееся их сбором и обработкой	любые физические лица
Основания охраны	закон	закон	регистрация	конфиденциальность	закон

Основания возникновения	сделка, наследование, реорганизация юридического лица, накоп-ление, переработка, результат использования и другое предус-мотренное законом	создание	установление режима доступа	от рождения
Сроки	до отчуждения, отказа и права, гибели или уничтожение имущества и другое предусмотренное законом	установлены законом или до отчуждения	устанавливаются собственником информации	пожизненно
Основания прекращения	отчуждение, отказ от права, гибель или уничтожение имущества и другое, предусмотренное законом	истечение срока или передача прав	когда информация становится общедоступной	по суду или с утратой дееспособности

Таблица 2.

Классификация защищаемой информации

Виды информации конфиденциального характера	Нормативные акты
Персональные данные	Федеральный закон "Об информации, информатизации и защите информации"
Тайна усыновления	Семейный кодекс Российской Федерации
Личная и семейная тайна	Гражданский кодекс Российской Федерации
Тайна следствия и судопроизводства	Уголовно-процессуальный кодекс Российской Федерации
Служебная тайна	Гражданский кодекс Российской Федерации
Служебная информация ограниченного распространения	Постановление Правительства Российской Федерации № 1233 от 3 ноября 1994 г.
Тайна связи	Федеральный закон "О связи"
Служебная информация	Федеральный закон "О рынке ценных бумаг"
Геологическая информация о недрах	Закон "О недрах"

Врачебная тайна	Основы законодательства Российской Федерации "Об охране здоровья граждан", Закон Российской Федерации "О трансплантации органов и (или) тканей человека"
Нотариальная тайна	Основы законодательства Российской Федерации "О нотариате"
Адвокатская тайна	Закон РСФСР "Об утверждении положения об адвокатуре"
Коммерческая тайна	Гражданский кодекс Российской Федерации
Банковская тайна	Гражданский кодекс Российской Федерации, Закон "О банках и банковской деятельности"
Тайна страхования	Гражданский кодекс Российской Федерации, Закон "О страховании"
"Ноу-хау"	Указ Президента России № 188 от 6 марта 1997г "Об утверждении перечня сведений конфиденциального характера"
Государственная тайна	Федеральный закон "О государственной тайне", Уголовный кодекс Российской Федерации

Межведомственной комиссией принят проект единой концепции информационной безопасности России, правовую основу которой составляют:

1. Конституция Российской Федерации.

2. Законы:

- "О безопасности";

- "О государственной тайне";

- "Об информации, информатизации и защите информации",

- "О коммерческой тайне";

- "О персональных данных".

Ключевым элементом концепции является отказ от взгляда на необходимость защиты только секретной информации и переход к осознанию необходимости защиты любого информационного ресурса, ценного для его владельца или собственника.

По оценке специалистов в сфере информации около 80% составляет беспатентная неавторизованная часть, т.е. та информация, которая может быть защищена классическими средствами патентного права. В то же время среди информации этого типа существует такая, которую можно, при определенных условиях, использовать во вред законным интересам граждан, субъектов хозяйственной деятельности, государства и общества.

В зависимости от типа защищаемых информационных ресурсов система обеспечения информационной безопасности должна создаваться на соответствующих правовых и организационных основах (рис. 1.).

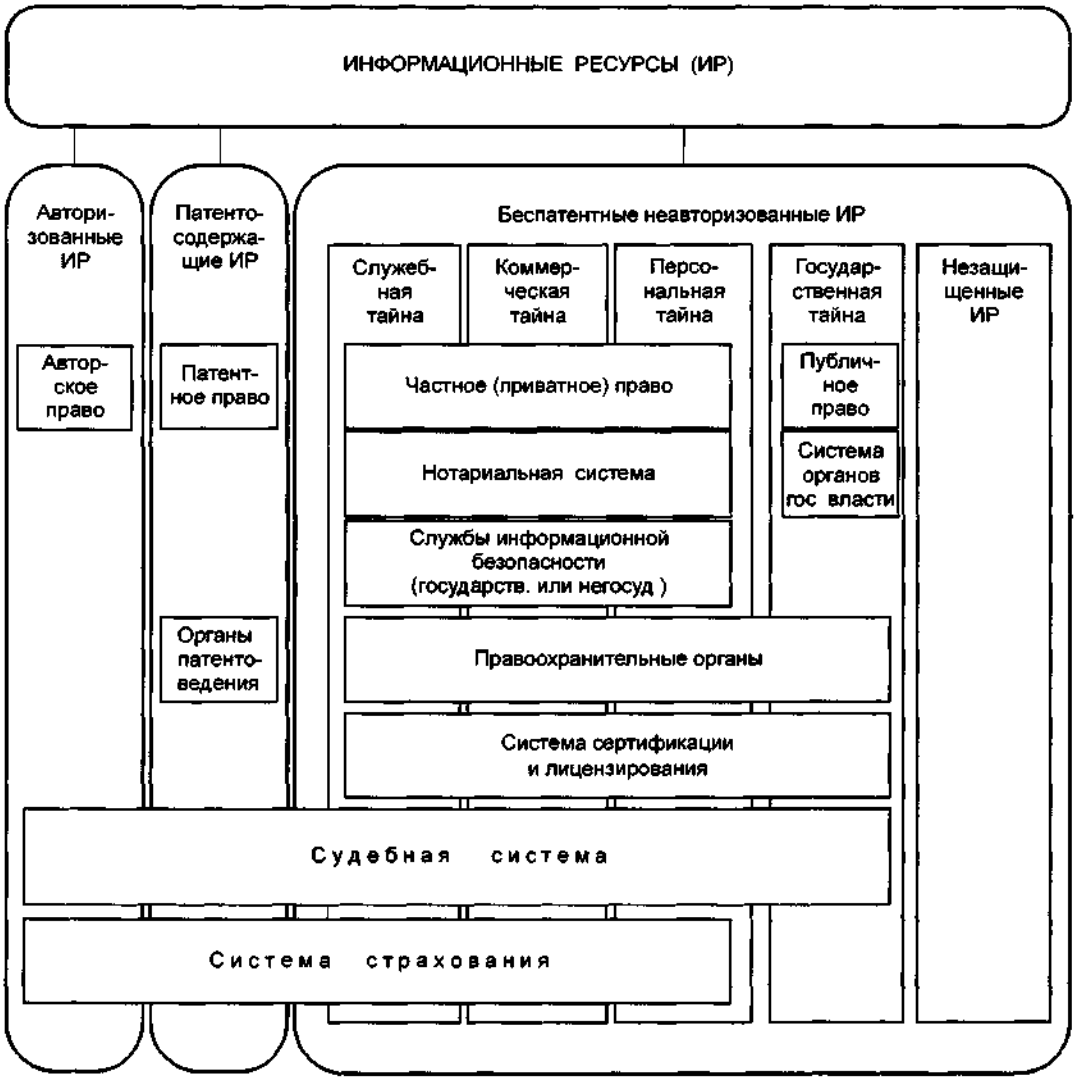


Рис. 1. Правовое и организационное обеспечение безопасности

Вопрос 3. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

3.1. Правовое регулирование и организация работ по защите информации

Вопросы развития и внедрения безопасных информационных технологий тесным образом связаны не только с решением научно-технических проблем, но и с вопросами правового регулирования общественных отношений в процессе информатизации. При этом их решение в большей степени зависит не только от уровня развития вычислительной техники, но и от признания за информацией статуса товара, продукта общественного производства. Установление в законодательном порядке права собственности на информацию является важнейшим аспектом формирования информационной политики государства.

Первым шагом в направлении создания правовых норм, закрепляющих права и обязанности граждан, коллективов и государства на информацию, явилось принятие Закона РФ "Об информации, информатизации и защите информации" (приложение к главе 4). В нем определен правовой режим информации, правила, процедуры и распределение ответственности в области защиты информации в системах ее обработки, установлен порядок правовой защиты и гарантии реализации прав и ответственности субъектов информационных взаимоотношений.

В области информатизации закон разработан как базовый для дальнейшего развития законодательства, разработки подзаконных актов и организационных структур в этой области.

Согласно упомянутому Закону "Об информации, информатизации и защите информации" (ст. 2), собственник информационных ресурсов - субъект, в полном объеме реализующий полномочия владения, пользования и распоряжения ими.

Информационные ресурсы (согласно ст. 6 того же Закона) могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности юридических и физических лиц. Отношения по поводу права собственности на информационные ресурсы регулируются в том числе и гражданским законодательством.

Правовой режим информационных ресурсов (ст. 4) определяется:

- порядком документирования информации;

- правами владения, пользования и распоряжения на отдельные документы и массивы документов в информационных системах;

- категорией информации по уровню доступа к ней;

- порядком правовой защиты информации.

Собственник информационных ресурсов (в соответствии с п. 7 ст.6 Закона) имеет закрепленное законодательством РФ право:

- назначать лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;

- устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

- определять условия распоряжения документами при их копировании и распространении.

Формирование рыночных экономических отношений в нашей стране совместно с поддержанием на должном уровне деятельности по обеспечению сохранности государственных секретов требует и усиленного внимания к вопросам промышленной и коммерческой тайны, так как институт коммерческой тайны является одновременно с авторским и патентным правом одной из правовых форм защиты интеллектуальной собственности.

В гл. 6 ГК РФ (ст. 128, 138) среди объектов гражданских прав преду-смотрена информация, результаты интеллектуальной деятельности, в том числе исключительные

права на них (интеллектуальная собственность), а также защита информации, составляющей служебную или коммерческую тайну (ст. 139).

Согласно ст. 139 действующего ГК РФ, информация составляет служебную или коммерческую тайну в случае, если она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам; к ней нет свободного доступа на законном основании; обладатель информации принимает меры к охране ее конфиденциальности. Эта статья ГК усиливает возможность запрета отнесения к коммерческой тайне тех или иных сведений, поскольку в ней содержится норма, согласно которой "сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом или иными правовыми актами", то есть и подзаконными в том числе.

Согласно этой же статье ГК РФ, лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе по контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Ст. 183 Уголовного кодекса РФ предусматривает уголовную ответственность за "незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну". При этом законодателем предусмотрены два состава преступления:

- собирание сведений, составляющих коммерческую или банковскую тайну;

- разглашение или использование указанных сведений без согласия владельца.

Собирание указанных сведений представляет собой формальный состав, т.е. для наступления уголовной ответственности достаточно самого факта собирания сведений, составляющих коммерческую или банковскую тайну независимо от наступления вредных последствий.

Уголовная ответственность за разглашение или использование подобных сведений без согласия владельца наступает в случае причинения указанными действиями крупного ущерба. Субъектами этого преступления являются лица, обладающие соответствующей информацией в связи со служебной или профессиональной деятельностью.

Из упомянутых правовых норм следует, что коммерческой тайной предприятия может быть все, что не запрещено законом или иными правовыми актами, охраняется предприятием и имеет ценность для предпринимательской деятельности, давая преимущество перед конкурентами, не владеющими ею.

Таким образом, фиксируется право собственника охранять свои интересы во взаимоотношениях со всеми субъектами рынка, включая государство. С юридическим закреплением понятия "коммерческая тайна" ко всему действующему массиву секретов в нашей стране, в том числе принадлежащих государству и им защищаемых (государственные секреты), добавился подмассив секретов, принадлежащих предприятию (служебные и коммерческие секреты), которые предприятие имеет право защищать, руководствуясь соображениями экономической безопасности и

конкурентной борьбы.

Реализация этого права осуществляется предприятием в соответствии со ст. 139, 421 ГК РФ путем создания и поддержания на договорной основе с другими физическими и юридическими лицами систем безопасности предприятия и защиты коммерческой информации, включающих в себя комплекс правовых, организационных, инженерно-технических, социально-психологических и иных мер, основывающихся на административно-правовых нормах РФ и организационно-распорядительных документах руководства предприятия (см. приложение к главе 5). Введение их в действие на предприятии приказом руководства является необходимым условием функционирования системы защиты коммерческой тайны, поскольку эти документы представляют собой основной пакет нормативных документов, регулирующих правовые отношения в процессе обеспечения безопасности и защиты его коммерческой тайны на предприятии.

Правовые аспекты защиты информации наиболее тесно связаны с вопросами организации работ и процедурами технологического процесса обработки информации.

Зарубежные исследования показывают, что несмотря на успехи от-дельных хакеров в проникновении в компьютерные системы и сети, большую опасность представляют законные пользователи этих систем и сетей, которые повинны в 80% правонарушений.

Учитывая то обстоятельство, что терминалами автоматизированных систем (АС), узлами сетей и даже отдельными ПЭВМ в нашей действительности пользуется большое количество официально допущенных к работе пользователей, задача поиска правонарушителя серьезно затрудняется.

Хотя в состав программного обеспечения АС, не говоря уже о современных системах защиты информации от несанкционированного доступа (НСД), входят средства контроля и протоколирования действий пользователя и посторонних лиц, доказать вину конкретного субъекта, предъявляя ему в качестве улики его идентификатор или пароль, достаточно сложно по двум причинам:

1) юридически очень сложно доказать, что эти атрибуты сохраняются в надлежащей тайне, к тому же пароли часто бывают групповыми;

2) такие улики и способ их нахождения не зафиксированы законодательно.

Указанными причинами и объясняется рост компьютерной преступности как со стороны хакеров, так и законных пользователей АС. Положение с организацией противодействия компьютерной преступности в настоящее время очень сложное, что обусловлено рядом причин:

- отсутствие опыта применения законодательства, предусматривающего административную, гражданскую, материальную и уголовную ответственность за компьютерные правонарушения;

- отсутствием должной координации деятельности по борьбе с компь-ютерной преступностью правоохранительных органов, специальных служб, органов суда и прокуратуры;

- отсутствием в системе правоохранительных органов, органах суда и прокуратуры

специально подготовленного состава, способного осуществлять выявление, предупреждение и пресечение компьютерных преступлений;

- отсутствием учета правонарушений, совершаемых с использованием средств информатизации;

- отсутствием необходимого технического и методического инструментария и опыта выявления и пресечения данного рода правонарушений;

- низким уровнем информационной и правовой культуры общества.

Любой закон будет действовать только при наличии механизма его реализации в виде организационных структур, обеспечивающих выполнение положений этого закона на всех уровнях управления.

Иерархическая структура управления деятельностью по обеспечению безопасности информации предусмотрена в Законе "Об информации, информатизации и защите информации" для координации, организационно-методического руководства деятельностью в этой области, контроля защищенности информации, осуществления других связанных с этим функций.

3.2. Административное регулирование вопросов защиты информации

Административное регулирование и практическая деятельность в области защиты информации в нашей стране была связана, в основном, с защитой государственных секретов в традиционной сфере обращения документов и в меньшей степени их защите при автоматизированной обработке.

В результате к концу 80-х годов сложилась ситуация, когда на государственном уровне отсутствовали утвержденные нормативно-технические требования по защите информации от НСД.

Единственным официальным документом, в очень общем виде определявшим требования в этой области, была инструкция по секретному делопроизводству, в ряде разделов которой содержались некоторые рекомендации по вопросам организации автоматизированной обработки информации. Это не означало, что в стране не занимались вопросами защиты от НСД, но организована эта работа была и координировалась на отраслевом уровне.

Для устранения этого недостатка Межведомственная комиссия осуществляет интеграцию, предусматривающую реализацию единой научно-технической политики по комплексной защите информации на всех уровнях управления силами Гостехкомиссии России. Таким образом, данная государственная система защиты информации осуществляет:

- координацию деятельности органов и организаций в области защиты информации, обрабатываемой техническими средствами;

- организационно-методическое руководство этой деятельностью, включая утверждение нормативно-технической документации;

- разработку и финансирование научно-технических программ по созданию средств

защиты информации;

- лицензирование деятельности предприятий по оказанию услуг в этой области;

- функции государственного органа по сертификации продукции по требованиям безопасности информации.

Государственная система защиты информации дополняется системой контроля защищенности информации в лице уполномоченных государством органов (Гостехкомиссией РФ), осуществляющих обязательный контроль за выполнением требований по защите информации, являющейся собственностью государства. Такие контрольные органы могут предоставлять для собственников негосударственной конфиденциальной информации услуги по оценке соответствия уровня защищенности этой информации установленным требованиям, о чем подробно написано в главе 19.

Необходимость существования государственной системы защиты информации и соответствующих организационных структур подтверждается не только в условиях так называемой административно-командной системы, но и в странах с развитыми рыночными отношениями. Зарождающаяся правовая основа защиты информации, приобретающая особенно большое значение в условиях сосуществования различных форм собственности, может опираться только на конкретные организационные структуры, осуществляющие законотворческую деятельность и являющиеся базой механизма реализации законов. Нельзя забывать, что и органы юстиции, являющиеся неотъемлемой принадлежностью любого государства, в случае противоправной деятельности по отношению к информации, должны опираться на определенные организационные структуры.

Важными элементами государственной системы защиты информации являются подсистемы лицензирования деятельности предприятий по оказанию услуг в области защиты информации и сертификации средств защиты информации. Функционирование указанных систем должно стимулировать разработку и внедрение современных, высококачественных технических средств и защитить потребителя продукции и услуг от недобросовестной работы исполнителя.

3.3. Система лицензирования

Система лицензирования направлена на создание условий, при которых право заниматься работами по защите информации для стороннего заказчика предоставлено только организациям, имеющим на этот вид деятельности соответствующее разрешение (лицензию). Это диктуется тем обстоятельством, что государственным и, в конечном счете, коммерческим структурам необходима доброкачественная продукция, действительно обеспечивающая защиту информации.

Система лицензирования в области защиты информации в настоящее время основана на Законе "О государственной тайне"; Положениях "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" и "О государственном лицензировании деятельности в области защиты информации".

В Законе "О государственной тайне" (ст. 27) вводится новая правовая норма - обязательное лицензирование деятельности предприятий, учреждений и организаций при их допуске к выполнению работ, связанных с использованием сведений, составляющих государственную тайну; к созданию средств защиты информации, а также к осуществлению мероприятий и оказанию услуг по защите государственной тайны.

Организационную структуру системы государственного лицензирования образуют:

- государственные органы по лицензированию;

- лицензионные центры;

- предприятия, претендующие на получение лицензии;

- предприятия-потребители услуг и продукции.

Следует отметить, что указанный пакет документов предусматривает в качестве обязательного условия функционирование этой системы на предприятиях государственного сектора, которая в то же время может быть использована по желанию потребителя и на предприятиях с другими формами собственности.

Согласно положениям, предприятие-заявитель, претендующее на получение лицензии, может обратиться с соответствующей заявкой в любой из лицензионных центров по отраслевому или региональному признаку и после обследования, проведенного экспертной комиссией, учитывающей техническую оснащенность предприятия-заявителя, опыт практической работы и готовность персонала, наличие нормативно-технических документов в выбранном направлении деятельности, получить лицензию на право оказания услуг сторонним предприятиям в этой области. При этом закрепляется также положение об обязательной государственной аттестации руководителей предприятий, ответственных за защиту сведений, составляющих государственную тайну.

Следует отметить, что на проведение работ по защите информации в собственных нуждах приобретение лицензии не требуется.

3.4. Система сертификации

Под сертификацией продукции на требования безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа-сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует требованиям стандартов по безопасности информации или иных нормативно-технических документов, утвержденных органом государственного управления в этой области (в настоящее время Гостехкомиссией РФ).

Система предусматривает сертификацию технических, программно-технических, программных средств, систем, сетей вычислительной техники, как законченной научно-технической продукции, средств защиты и контроля эффективности защиты по требованиям безопасности информации.

Основные принципы, организационная структура системы сертификации продукции по требованиям безопасности информации, а также правила проведения сертификации этой продукции изложены в "Положении о сертификации средств защиты информации".

Положение о сертификации средств защиты определяет.

1) структуру, взаимоотношения и права организаций, специализирующихся в области защиты информации;

2) необходимый комплекс сведений при решении двух практических задач, организации сертификации разработанных средств защиты; целесообразности заключения договоров о разработке и покупке средств защиты информации.

Система сертификации продукции по требованиям безопасности информации направлена на: обеспечение прав собственника и владельца информации (владельца автоматизированной системы); сохранение в тайне информации, обрабатываемой средствами вычислительной техники; исключение несанкционированного ее искажения или уничтожения; поддержание АС в управляемом состоянии. Она призвана обеспечить потребителям средств вычислительной техники (СВТ) и АС безопасную обработку любой конфиденциальной или иной ценной информации.

В то же время при реализации эта система требует объективности и независимости проведения испытаний образцов продукции и экспертизы результатов таких испытаний. Это возможно при выполнении следующих условий: наличия постоянного совершенствования нормативно-технических документов, определяющих требования к характеристикам защищенности продукции, использования в процессе испытаний сертифицированных тестовых средств при строгом соблюдении предписанных правил и процедур.

Следует отметить, что и в вопросах сертификации продукции в целом, в сертификации СВТ по требованиям безопасности информации мы значительно отстали от развитых зарубежных стран. В США, например, для обработки секретной и несекретной информации правительственных ведомств и фирм-подрядчиков Пентагона используется только сертифицированная по требованиям безопасности национальных стандартов программно-техническая продукция. В этих целях публикуются соответствующие каталоги защищенных СВТ, и на рынок поставляются серийные защищенные изделия.

3.5. Страхование информационных систем

Все более широкие слои общества пользуются услугами сберегательного банка, коммерческих банков, инвестиционных фондов, трастовых компаний, финансово-промышленных групп и других государственных и частных финансово-кредитных организаций. Для удовлетворения возрастающих потребностей общества в услугах финансовые учреждения постоянно совершенствуют свою работу в части внедрения современных технических и программных средств вычислительной техники, информационных систем и коммуникационных сетей передачи информации.

Использование эффективных информационных технологий обеспечивает огромные

преимущества в процессе передачи, хранения и обработки потоков информации.

Такое положение, связанное с освоением современных информационных технологий, потенциально создает предпосылки для возникновения риска утраты важной государственной информации за счет ошибок, возникающих в технических и программных средствах вычислительной техники, ошибок и неквалифицированных действий обслуживающего персонала, несанкционированного действия третьих лиц, других причин. Имеются случаи воздействия "электронного пиратства" на сферу кредитно-финансовых банковских компьютерных систем.

С ростом и интеграцией компьютерных сетей (масштаба фирмы, банка, предприятия, города, региона), с появлением распределенных кредитно-финансовых сетей электронного межбанковского клиринга, программ типа "Клиент-Банк" и других прикладных коммуникационных систем возможные потери могут возрастать.

Статистика показывает, что среди информационных преступлений 30% составляют раскрытие пароля, 22% - несанкционированный доступ, 44% - программные закладки, включая "вирусы", и 2% - воздействие извне системы. Утечка только 20% информации ведет к разорению 65% фирм и компаний.

По некоторым оценкам, в прошлом году российская компьютерная индустрия потеряла из-за пиратства 75 млн. дол.

Поэтому информационная безопасность компьютерных систем и коммуникаций приобретает особую роль и становится одним из важнейших аспектов деятельности государственных и коммерческих организаций.

Информационная безопасность может быть достигнута в результате использования организационных мер защиты, а также программно-аппаратных комплексов защиты каналов связи, компьютерных систем и данных.

Однако информационную систему нужно не только эффективно защитить, но и убедить в надежности ее пользователей. Очевидно, и опыт это доказывает, достигнуть 100% безопасности информации практически невозможно. Если система незащищена, риск потери информации составляет 50-60%. Введение парольной защиты, разграничения доступа, криптографии снижает риск до 30%, использование технических средств защиты от несанкционированных действий - 10%. Снижение риска до 1 % (умышленные действия обслуживающего персонала) достигается полной изоляцией информационной системы или компьютера.

Следовательно, имеется реальная возможность наступления непредвиденного события (страхового случая), влекущего за собой потерю работоспособности сложных электронных систем, утрату конфиденциальной информации и потерю дохода.

Исходя из вышеизложенного и предположив, что наступление риска потери информации носит случайный характер, не зависящий от воли владельца информации, закономерно усиливается интерес к страхованию собственников и пользователей информационных систем, информационных ресурсов, технических и программных средств вычислительной техники.

Становление и постепенное расширение рыночных отношений коренным образом меняет место и роль страхования в защите экономических и информационных

интересов предприятий и предпринимателей, объективно привязывают предпринимателей к страхованию.

Плата за страхование - страховые взносы есть плата за риск, плата за спокойствие в хозяйственной жизни.

Именно страховая компания, которая покроет риски финансового института, вкладчиков и разработчика информационной системы может стать гарантом информационной безопасности.

Интерес к страхованию усиливается и высокой степенью возникновения пожаров, аварий, нарастанием криминогенной обстановки. Государственная либо коммерческая организация, обеспечивая безопасность информации, в том числе страхованием информационных рисков, привлекает этим клиентов, повышает надежность информационных систем и получает дополнительную прибыль.

В условиях рыночных отношений особенно актуальной становится проблема обязательной и добровольной формы страхования. К приоритетным относятся те объекты (обязательное страхование), гибель которых задевает не только интересы страхователей, но и всего общества.

При обязательном страховании почти на одну треть снижаются размеры страховых выплат в связи со сплошным охватом объектов страхования.

Указом Президента от 6 апреля 1994 г. "Об основных направлениях государственной политики в сфере обязательного страхования" установлено, что при разработке проектов законов РФ по данным вопросам обязательного страхования должно обеспечиваться первоочередное правовое урегулирование видов, непосредственно направленных на защиту прав и свобод человека и гражданина, гарантированных Конституцией РФ.

Одной из форм возмещения ущерба является страховая защита в виде обязательного страхования информационных рисков.

Обязательное страхование становится необходимым тогда, когда наносимый страховыми случаями ущерб задевает интересы не только страхователя, но и государства, всего общества.

При этом и страховщики и страхователи обязаны в силу закона участвовать в проведении соответствующих видов страхования.

Понимая, что интересы граждан только тогда надежно защищены, когда существует механизм возмещения информационных рисков, связанных с информационной безопасностью, можно создать специализированную страховую компанию по страхованию информационных рисков.

К информационным рискам относятся риски, связанные с потерей или искажением информации в компьютерах, сетях и системах в результате:

- отказов, сбоев технических и программных средств;

- внедрения "вирусов";

- неумышленных действий обслуживающего персонала;

- несанкционированных действий;

- утечки информации за счет побочных электромагнитных излучений и наводок.

Субъектами страхования (страхователями) могут выступать Сбербанк России и его филиалы, коммерческие банки, акционерные общества, ассоциации, корпорации, государственные организации, учреждения и пользователи (информационных систем, информационных ресурсов, систем автоматизации банковской деятельности, автоматизации офисов, систем и сетей автоматизации повседневной деятельности, систем обработки документооборота, программных и технических средств вычислительной техники).

Объем страхового поля определяется количеством средств вычислительной техники и программного обеспечения, имеющихся у пользователей. В настоящее время объем страхового поля по компьютерам составляет $3.6 млрд. Учитывая, что стоимость программного обеспечения составляет ориентировочно 50% и не все компьютеры объединены в сети, объем страхового поля следует увеличить на $1.8 млрд. Общий объем страхового поля составляет $5.4 млрд.

При охвате 5% страхового поля страховая сумма составит $270 млн. При среднем тарифе 2% страховой взнос равен $5.4 млн.

Через систему страхования перераспределяется только до 2,8% валового продукта Российской Федерации, что почти в 4 раза меньше уровня индустриально развитых стран Западной Европы, США и Японии.

Учитывая, что информационные системы охватывают всю территорию России, имеется возможность к неуклонному расширению сферы деятельности, к постоянному увеличению числа страхователей, к расширению территории деятельности, к открытию и функционированию филиалов страховой компании на местах.

Это дает предпосылки для эффективного проведения страховых операций и создания необходимых резервов для осуществления выплат по страховым случаям, а также получения прибыли.

Вывод: в настоящих условиях хаотичного рынка средств защиты информации целесообразно придерживаться следующих правил:

1. Прежде чем заключать деловые контакты о разработке или покупке средств защиты у сторонних организаций необходимо выяснить: имеет ли данная организация лицензию на выполнение работ по защите информации, какой вид деятельности разрешен, и соответствует ли он данной работе, не просрочена ли лицензия.

2. При наличии правильно оформленной лицензии необходимо проанализировать сертификат на средство защиты, определить, кем он выдан, когда и какие проводились испытания средства защиты информации, при каких условиях данное средство защиты будет нормально функционировать.

Выполнение указанных правил позволит избежать возможных неприятностей по обеспечению информационной безопасности и правильно использовать средство защиты.

ЛЕКЦИЯ 3
ТРЕБОВАНИЯ РУКОВОДЯЩИХ ДОКУМЕНТОВ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И НСД

Учебные вопросы:

1. Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»)
2. Европейские критерии по обеспечению ИБ

Вопрос 1. КРИТЕРИИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ МИНИСТЕРСТВА ОБОРОНЫ США

(«ОРАНЖЕВАЯ КНИГА»)

«Критерии безопасности компьютерных систем» («Trusted Computer System Evaluation Criteria») [1], получившие неформальное название «Оранжевая книга», были разработаны Министерством обороны США в 1983 году с целью определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработки соответствующей методологии анализа политики безопасности, реализуемой в компьютерных системах военного назначения.

В данном документе были впервые нормативно определены такие понятия, как «политика безопасности», ТСВ и т. д. Согласно «Оранжевой книге, безопасная компьютерная система — это система, поддерживающая управление доступом к обрабатываемой в ней информации такое, что только соответствующим образом уполномоченные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию. Предложенные в этом документе концепции защиты и набор функциональных требований послужили основой для формирования всех появившихся впоследствии стандартов безопасности.

Требования и критерии «Оранжевой книги»

В «Оранжевой книге» предложены три категории требований безопасности — политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены непосредственно на обеспечение безопасности информации, а два последних — на качество самих средств защиты (рисунок 1). Рассмотрим эти требования подробнее.

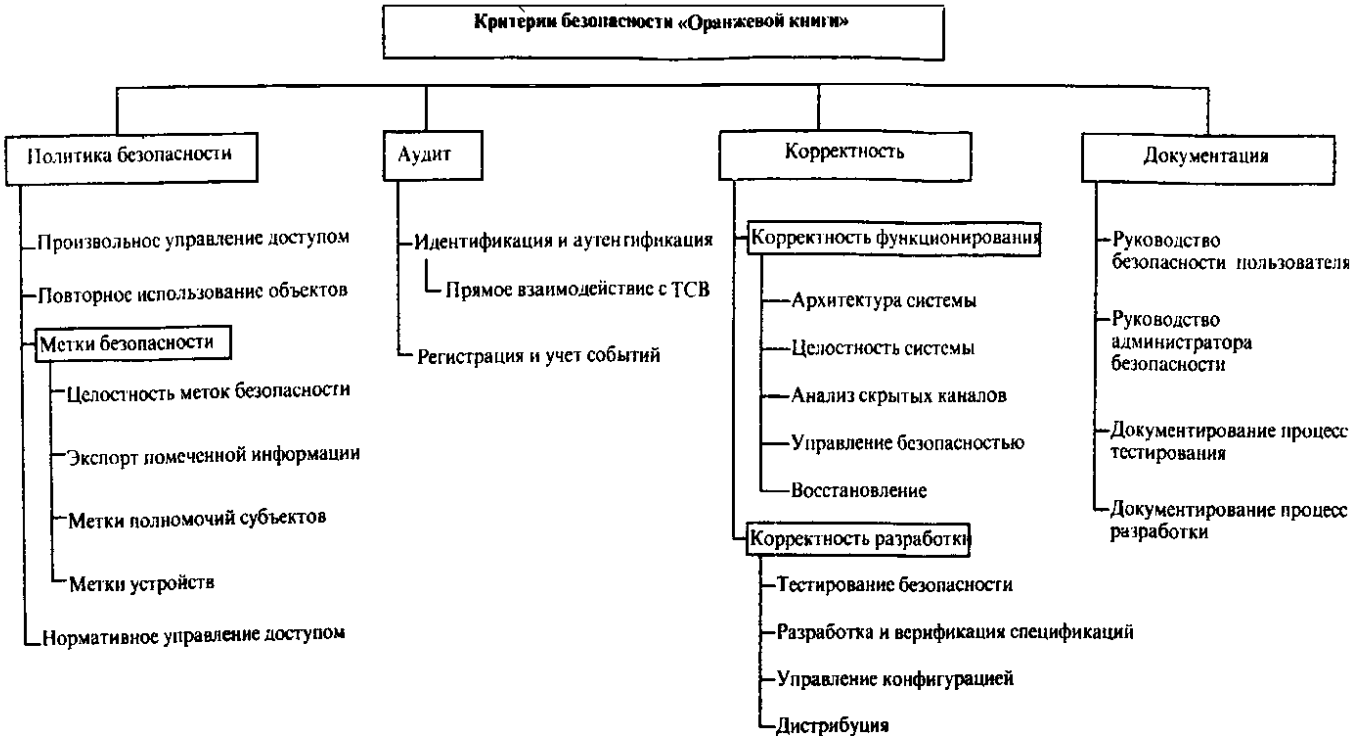


Рисунок 1. Критерии безопасности

Политика безопасности

Требование 1. Политика безопасности

Система должна поддерживать точно определенную политику безопасности. Возможность осуществления субъектами доступа к объектам должна определяться на основании их идентификации и набора правил управления доступом. Там, где необходимо, должна использоваться политика нормативного управления доступом, позволяющая эффективно реализовать разграничение доступа к категорированной информации (информации, отмеченной грифом секретности, типа «секретно». «совершенно секретно» и т.д.).

Требование 2. Метки

С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа. Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

Аудит

Требование 3. Идентификация и аутентификация

Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными

компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

Требование 4. Регистрация и учет

Для определения степени ответственности пользователей за действия а системе, все происходящие в ней события. имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событии и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективности его анализа. Протокол событии должен быть надежно защищен от несанкционированного доступа, модификации или уничтожения.

Корректность

Требование 5. Контроль корректности функционирования средств защиты

Средства защиты должны содержать независимые аппетитные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находится под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

Требование 6. Непрерывность защиты

Все средства защиты (в т.ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

Рассматриваемые далее критерии безопасности компьютерных систем представляют собой конкретизацию данных обобщенных требований.

Критерии безопасности

Приведенные выше базовые требования к безопасности служат основой для критериев, образующих единую шкалу оценки безопасности компьютерных систем, определяющую семь классов безопасности.

«Оранжевая книга» предусматривает четыре группы критериев, которые соответствуют различной степени защищенности: от минимальной (группа D) до формально доказанной (группа A). Каждая группа включает один или несколько классов. Группы D и A содержат по одному классу (классы D1 и A1 соответственно), группа C — классы Cl, C2, а группа B — Bl, B2, B3, характеризующиеся различными

наборами требований безопасности. Уровень безопасности возрастает при движении от группы D к группе A, а внутри группы — с возрастанием номера класса.

Группа D. Минимальная защита

* Класс D1. Минимальная защита. К этому классу относятся все системы, которые не удовлетворяют требованиям других классов.

Группа C. Дискреционная защита

Группа C характеризуется наличием произвольного управления доступом и регистрацией действий субъектов.

* Класс C1. Дискреционная защита. Системы этого класса удовлетворяют требованиям обеспечения разделения пользователей и информации и включают средства контроля и управления доступом, позволяющие задавать ограничения для индивидуальных пользователей, что дает им возможность защищать свою приватную информацию от других пользователей. Класс C1 рассчитан на многопользовательские системы, в которых осуществляется совместная обработка данных одного уровня секретности.

* Класс C2. Управление доступом. Системы этого класса осуществляют более избирательное управление доступом. чем системы класса C1, с помощью применения средств индивидуального контроля за действиями пользователей, регистрацией, учетом событий и выделением ресурсов.

Группа B. Мандатная защита

Основные требования этой группы — нормативное управление доступом с использованием меток безопасности, поддержка модели и политики безопасности, а также наличие спецификаций на функции TCB. Для систем этой группы монитор взаимодействий должен контролировать все события в системе.

* Класс B1. Защита с применением меток безопасности.

Системы класса B1 должны соответствовать всем требованиям, предъявляемым к системам класса C2, и, кроме того должны поддерживать определенную неформально модель безопасности, маркировку данных и нормативное управление доступом. При экспорте из системы информация должна подвергаться маркировке. Обнаруженные в процессе тестирования недостатки должны быть устранены.

* Класс B2. Структурированная защита. Для соответствия классу B2 TCB системы должно поддерживать формально определенную и четко документированную модель безопасности, предусматривающую произвольное и нормативное управление доступом, которое распространяется по сравнению с системами класса B1 на все субъекты. Кроме того, должен осуществляться контроль скрытых каналов утечки информации. В структуре TCB должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс TCB должен быть четко определен а его архитектура и реализация должны быть выполнены с учетом возможности проведения тестовых испытаний. По сравнению с классом B1 должны быть усилены средства аутентификации. Управление безопасностью осуществляется администраторами системы. Должны быть предусмотрены средства управления конфигурацией.

* Класс B3. Домены безопасности. Для соответствия ЭТОМУ классу TCB системы должно поддерживать монитор взаимодействий, который контролирует все типы доступа субъектов к объектам и который невозможно обойти Кроме того. TCB должно быть структурировано с целью исключения из него подсистем, не отвечающих за реализацию функций защиты, и быть достаточно компактно для эффективного тестирования и анализа. В ходе разработки и реализации TCB должны вменяться методы и средства, направленные на минимизацию его сложности Средства аудита должны включать механизмы оповещения администратора при возникновении событий, имеющих значение для безопасности системы. Требуется наличие средств восстановления работоспособности системы.

Группа A. Верифицированная защита

Данная группа характеризуется применением формальных методов верификации корректности работы механизмов управления доступом (произвольного и нормативного). Требуется дополнительная документация, демонстрирующая, что архитектура и реализация TCB отвечают требованиям безопасности.

* Класс A1. Формальная верификация. Системы класса A1 функционально эквивалентны системам класса B3, и к ним не предъявляется никаких дополнительных функциональных требований. В отличие от систем класса B3 в ходе разработки должны применяться формальные методы верификации, что позволяет с высокой уверенностью получить корректную реализацию функций защиты. Процесс доказательства адекватности реализации начинается на ранней стадии разработки с построения формальной модели политики безопасности и спецификаций высокого уровня. Для обеспечения методов верификации системы класса A1 должны содержать более мощные средства управления конфигурацией и защищенную процедуру дистрибуции.

Приведенные классы безопасности определили основные концепции безопасности и ход развития средств защиты.

Интерпретация и развитие «Оранжевой книги»

Опубликование «Оранжевой книги» стало важным этапом и сыграло значительною роль в развитии технологий обеспечения безопасности компьютерных систем. Тем не менее в ходе применения ее положений выяснилось, что часть практически важных вопросов осталась за рамками данного стандарта и, кроме того, с течением времени (с момента опубликования прошло шестнадцать лет) ряд положений устарел и потребовал пересмотра.

Круг специфических вопросов по обеспечению безопасности компьютерных сетей и систем управления базами данных нашел отражение в отдельных документах, изданных Национальным центром компьютерной безопасности США в виде дополнений к «Оранжевой книге» — «Интерпретация «0ранжевой книги» для компьютерных сетей» («Trusted Network Interpretation» [2]) и «Интерпретация «Оранжевой книги» для систем управления базами данных» («Trusted Database Management System Interpretation» [3]). Эти документы содержат трактовку основных положений «Оранжевой книги» применительно к соответствующим классам систем обработки информации.

Потеря актуальности рядом положении «Оранжевой книги» вызвана прежде всего интенсивным развитием компьютерных технологий и переходом с мэйнфреймов (типа вычислительных комплексов IBM-360, 370; советский аналог — машины серии ЕС) к рабочим станциям, высокопроизводительным персональным компьютерам и сетевой модели вычислений. Именно для того, чтобы исключить возникшую в связи с изменением аппаратной платформы некорректность некоторых положений «Оранжевой книги», адаптировать их к современным условиям и сделать адекватными нуждам разработчиков и пользователей программного обеспечения, и была проделана огромная работа по интерпретации и развитию положений этого стандарта. В результате возник целый ряд сопутствующих «Оранжевой книге» документов, многие их которых стали ее неотъемлемой частью. К наиболее часто упоминаемым относятся:

* Руководство по произвольному управлению доступом в безопасных системах («A guide to understanding discretionary access control in trusted systems») [4].

* Руководство по управлению паролями («Password management guideline») [5].

* Руководство по применению Критериев безопасности компьютерных систем в специфических средах («Guidance for applying the Department of Defence Trusted Computer System Evaluation Criteria in specific environment») [6].

* Руководство по аудиту в безопасных системах (<Guide to Under-standing Audit in Trusted Systems») [7].

* Руководство по управлению конфигурацией в безопасных системах («Guide to understanding configuration management in trusted systems) [8].

Количество подобных вспомогательных документов, комментариев и интерпретаций значительно превысило объем первоначального документа, и в 1995 году Национальным центром компьютерной безопасности США был опубликован документ под названием «Пояснения к критериям безопасности компьютерных систем», объединяющий все дополнения и разъяснения. При его подготовке состав подлежащих рассмотрению и толкованию вопросов обсуждался на специальных конференциях разработчиков и пользователей защищенных систем обработки информации. В результате открытого обсуждения была создана база данных, включающая все спорные вопросы, которые затем в полном объеме были проработаны специально созданной рабочей группой. В итоге появился документ, объединивший все изменения и дополнения к «Оранжевой книге», сделанные с момента ее опубликования, что привело к обновлению стандарта и позволило применять его в современных условиях.

Выводы: «Критерии безопасности компьютерных систем» министерства обороны США представляют собой первую попытку создать единый стандарт безопасности, рассчитанный на разработчиков, потребителей и специалистов по сертификации компьютерных систем. В свое время этот документ явился настоящим прорывом в области безопасности информационных технологий и послужил отправной точной для многочисленных исследований и разработок. Основной отличительной чертой этого документа является его ориентация на системы военного применения, в основном на операционные системы. Это предопределило доминирование требований, направленных на обеспечение секретности обрабатываемой информации и

исключение возможностей ее разглашения. Большое внимание уделено меткам (грифам секретности) и правилам экспорта секретной информации.

При этом критерии адекватности реализации средств защиты и политики безопасности отражены слабо, соответствующий раздел ограничивается требованиями контроля целостности средств защиты и поддержания их работоспособности, чего явно недостаточно.

Высший класс безопасности, требующий осуществления верификации средств защиты, построен на доказательстве соответствия программного обеспечения его спецификациям с помощью специальных методик, однако это доказательство (очень дорогостоящее, трудоемкое и практически неосуществимое для реальных операционных систем) не подтверждает корректность и адекватность реализации политики безопасности.

«Оранжевая книга» послужила основой для разработчиков всех остальных стандартов информационной безопасности и до сих пор используется в США в качестве руководящего документа при сертификации компьютерных систем обработки информации.

Вопрос 2. ЕВРОПЕЙСКИЕ КРИТЕРИИ ПО ОБЕСПЕЧЕНИЮ ИБ

Проблемы информационной безопасности актуальны не только для Соединенных Штатов. Вслед за выходом «Оранжевой книги» страны Европы совместно разработали общие «Критерии безопасности информационных технологий» («Information Technology Security Evaluation Criteria», далее «Европейские критерии») [9]. Данный обзор основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран: Франции, Германии, Нидерландов и Великобритании.

Основные понятия

«Европейские критерии» рассматривают следующие задачи средств информационной безопасности:

• защита информации от несанкционированного доступа с целью обеспечения конфиденциальности;

• обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;

• обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

Для того чтобы удовлетворить требованиям конфиденциальности, це-лостности и работоспособности, необходимо реализовать соответствующий набор функций безопасности, таких, как идентификация и аутентификация, управление доступом, восстановление после сбоев и т. п. Чтобы средства за-щиты можно было признать эффективными, требуется определенная степень уверенности в правильности их

выбора и надежности функционирования. Для решения этой проблемы в «Европейских критериях» впервые вводится понятие адекватности (assurance) средств защиты.

Адекватность включает в себя два аспекта: эффективность, отражающую соответствие средств безопасности решаемым задачам, и корректность, характеризующую процесс их разработки и функционирования. Эффективность определяется соответствием между задачами, поставленными перед средствами безопасности, и реализованным набором функций защиты — их функциональной полнотой и согласованностью, простотой использования, а также возможными последствиями использования злоумышленниками слабых мест защиты. Под корректностью понимается правильность и надежность реализации функций безопасности.

Общая оценка уровня безопасности системы складывается из функциональной мощности средств защиты и уровня адекватности их реализации.

Функциональные критерии

В «Европейских критериях» средства, имеющие отношение к информационной безопасности, рассматриваются на трех уровнях детализации. На первом уровне рассматриваются цели, которые преследует обеспечение безопасности, второй уровень содержит спецификации функций защиты, а третий — реализующие их механизмы. Спецификации функций защиты предлагается рассматривать с точки зрения следующих требований:

• идентификация и аутентификация;

• управление доступом;

• подотчетность;

• аудит;

• повторное использование объектов;

• целостность информации;

• надежность обслуживания;

• безопасность обмена данными.

Большинство из перечисленных требований совпадает с аналогичными требованиями «Оранжевой книги». Остановимся лишь на специфичных для «Европейских критериев» моментах.

Требования безопасности обмена данными регламентируют работу средств, обеспечивающих безопасность данных, передаваемых по каналам связи, и включают следующие разделы:

• аутентификация;

• управление доступом;

• конфиденциальность данных;

• целостность данных:

• невозможность отказаться от совершенных действий.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы-шаблоны. В «Европейских критериях» таких классов десять. Пять из них (F-C1, F-C2, F-B1, F-B2, F-B3) соответствуют классам безопасности «Оранжевой книги» с аналогичными обозначениями. Рассмотрим подробнее другие пять классов, так как их требования отражают точку зрения разработчиков стандарта на проблему безопасности.

Класс F-IN предназначен для систем с высокими потребностями в обеспечении целостности, что типично для систем управления базами данных. Его описание основано на концепции «ролей», соответствующих видам деятельности пользователей, и предоставлении доступа к определенным объектам только посредством доверенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, создание, переименование и выполнение объектов.

Класс F-AV характеризуется повышенными требованиями к обеспечению работоспособности. Это существенно. например, для систем управления технологическими процессами. В требованиях этого класса указывается, что система должна восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции постоянно оставались доступными. В таком же режиме должна происходить и замена компонентов системы. Независимо от уровня загрузки должно гарантироваться определенное время реакции системы на внешние события.

Класс F-DI ориентирован на распределенные системы обработки информации. Перед началом обмена и при получении данных стороны должны иметь возможность провести идентификацию участников взаимодействия и проверить ее подлинность. Должны использоваться средства контроля и исправления ошибок. В частности, при пересылке данных должны обнаруживаться все случайные или намеренные искажения адресной и пользовательской информации. Знание алгоритма обнаружения искажений не должно позволять злоумышленнику производить нелегальную модификацию передаваемых данных. Должны обнаруживаться попытки повторной передачи ранее переданных сообщений.

Класс F-DC уделяет особое внимание требованиям к конфиденциально-сти передаваемой информации. Информация по каналам связи должна передаваться в зашифрованном виде. Ключи шифрования должны быть защищены от несанкционированного доступа.

Класс F-DX предъявляет повышенные требования и к целостности и к конфиденциальности информации. Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования и защиты от анализа трафика. Должен быть ограничен доступ к ранее переданной информации, которая, в принципе может способствовать проведению криптоанализа.

Критерии адекватности

«Европейские критерии» уделяют адекватности средств защиты значительно больше внимания, чем функциональным требованиям. Как уже говорилось адекватность

складывается из двух компонентов — эффективности и корректности работы средств защиты. Для оценки степени адекватности используются следующие критерии (рисунок 2).

Рисунок 2. Критерии адекватности

«Европейские критерии» определяют семь уровней адекватности — от E0 до E6 (в порядке её возрастания). Уровень E0 обозначает минимальную адекватность (аналог уровня D «Оранжевой книги»). При проверке адекватности анализируется весь жизненный цикл системы — от начальной фазы проектирования до эксплуатации и сопровождения. Уровни адекватности от E1 до E6 выстроены по нарастанию требований тщательности контроля. Так, на уровне E1 анализируется лишь общая архитектура системы, а адекватность средств защиты подтверждается функциональным тестированием. На уровне E3 к анализу привлекаются исходные тексты программ и схемы аппаратного обеспечения. На уровне E6 требуется формальное описание функций безопасности, общей архитектуры, а также политики безопасности.

Степень безопасности системы определяется самым слабым из критически важных механизмов защиты. В «Европейских критериях» определены три уровня безопасности — базовый, средний и высокий. Безопасность считается базовой, если средства защиты способны противостоять отдельным случайным атакам. Безопасность считается средней, если средства защиты способны противостоять злоумышленникам, обладающим ограниченными ресурсами и возможностями. Наконец, безопасность можно считать высокой, если есть уверенность, что средства защиты могут быть преодолены только злоумышленником с высокой квалификацией. набор возможностей и ресурсов которого выходит за рамки разумного.

Выводы: «Европейские критерии безопасности информационных технологий», появившиеся вслед за «Оранжевой книгой», оказали существенное влияние на

стандарты безопасности и методику сертификации.

Главное достижение этого документа — введение понятия адекватности средств защиты и определение отдельной шкалы для критериев адекватности. Как уже упоминалось, «Европейские критерии» придают адекватности средств защиты даже большее значение, чем их функциональности. Этот подход используется во многих появившихся позднее стандартах информационной безопасности. Необходимо отметить, что «Европейские критерии» тесно связаны с «Оранжевой книгой», что делает их не вполне самостоятельным документом. На первый взгляд довольно странным выглядит тот факт, что «Европейские критерии» признают возможность наличия недостатков в сертифицированных системах (критерий возможности использования недостатков защиты), однако на самом деле это свидетельствует о трезвом взгляде на существующее положение и признании того очевидного факта, что реальные системы еще весьма несовершенны и далеки от идеала.

«Европейские критерии» безопасности информационных технологий, наряду с «Оранжевой книгой» легли в основу многих стандартов безопасности компьютерных систем.

ЛЕКЦИЯ 4
ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Учебные вопросы:

1. Создание концепции зашиты.

2. Правовые основы деятельности Службы безопасности

3. Функции, задачи и особенности деятельности Службы безопасности Организационные мероприятия и процедуры по обеспечению защиты информации в автоматизированных системах

Введение

Обеспечение комплексной защиты объектов является индивидуальной задачей, что обусловлено экономическими соображениями, состоянием, в котором находится объект защиты (стадии разработки, внедрения, эксплуатации), и рядом других обстоятельств. В предыдущих занятиях на основе анализа современного состояния проблемы защиты были сформулированы основные принципы защиты хозяйствующих субъектов. Необходимо обобщить их на концептуальном уровне для того, чтобы определить общую структуру службы безопасности (СБ), которая в конечном счете и создает СЗ. Поэтому в данной главе изложена концептуальная сторона проблемы обеспечения безопасной деятельности коммерческих предприятий и фирм на примере обеспечения безопасности банка.

Вопрос. 1 СОЗДАНИЕ КОНЦЕПЦИИ ЗАШИТЫ

1.1. Основные положения

Во всех своих действиях и делах любое предприятие подчинено одному общему принципу - выживай. Наградой за действия, способствующие выживанию, является стабилизация или увеличение прибыли, наказанием за разрушительные действия (внутренние или внешние) становится уменьшение прибыли или прекращение коммерческой деятельности банка.

Выживание любого объекта защиты зависит от двух составляющих:

1) экономической деятельности;

2) экономической безопасности.

Оптимальным решением любой проблемы, стоящей перед объектом защиты, в первою очередь банком, является то, которое приносит макси-мальную пользу обеим

составляющим. Что могло бы служите оптимальной характеристикой выживания различных банков? Они должны иметь различные фундаментальные основы, которые были бы неодинаковы у разных банков, так же, как одна окружающая среда отличается от другой. Однако в одной среде существует некоторое количество банков. Поэтому между ними существует борьба за выживание - конкуренция. Аналогией вышесказанному является экологический "закон Гаузе", формулировка которого следующая: никакие два вида, имеющие сходные экологические потребности, не могут в течение длительного времени сосуществовать в одном и в том же местообитании. Если два вида идентичны (или если один представитель одного вида идентичен представителям другого вида по нескольким характеристикам), то ни одна экосистема, в которую входят оба эти вида, не может быть устойчивой.

Таким образом, деятельность СБ направлена на поддержание выживания банка путем сохранения или получения максимальной прибыли за счет минимизации ущерба от внешних и внутренних разрушительных воздействий. Это может достигаться только при активном противодействии внешним и внутренним угрозам безопасности, т.е. формированию внешней и внутренней благоприятной атмосферы безопасности коммерческой деятельности в условиях конкуренции.

Прежде чем приступить к созданию СЗ, необходимо определить объекты защиты, чье уничтожение, модификация или несанкционированное использование может привести к уменьшению прибыли. Определив объекты защиты, следует выявить среды их существования и возможные формы. Данный анализ позволяет определить множество угроз безопасности защищаемых объектов. Зная возможные угрозы, можно предположить частоту данных угроз, а затем выбрать адекватные средства и методы защиты. Данный алгоритм показан на рис 1.

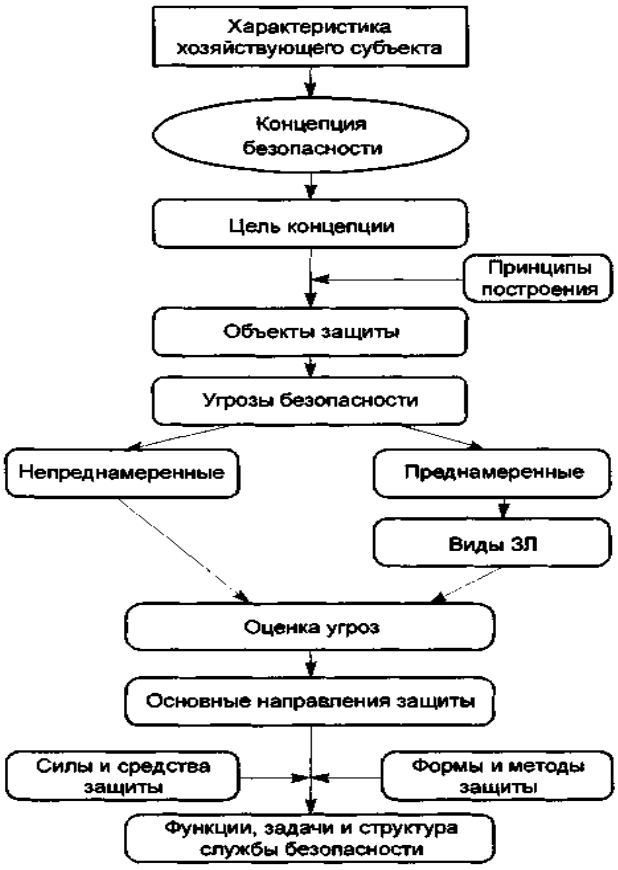


Рис. 1 Подход к созданию СБ

Предложенный алгоритм обусловлен тем, что в подавляющем числе случаев в процессе защиты присутствуют два субъекта: нападающий и обороняющийся, причем второй находится в состоянии неопределенности о возможных действиях первого в большей степени, т.к. он не является инициирующей стороной. Кроме того, процесс защиты еще более осложняется наличием "человеческого фактора" с обеих сторон. Конечной целью создания СЗ является разработка защищенных технологий, обеспечивающих заданный уровень защиты при минимальной стоимости средств и методов защиты для всех функциональных подразделений объекта защиты.

1.2. Оценка угроз безопасности

Проведем оценку угроз безопасности.

Для того, чтобы риск деятельности банка из-за внешней и внутренней обстановки был бы минимальным, необходимо выполнить оценку степени возможных преднамеренных и непреднамеренных угроз, которая должна производиться из учета следующих факторов:

1) возможного ущерба, вызванного действием угрозы;

2) использования результатов отечественной и мировой статистики;

3) внешней и внутренней обстановки;

4) результатами собственной статистики.

Определенная объективность в оценке степени угроз может быть достигнута путем детального анализа функционирования банка и использования независимых экспертных оценок экспертов, специализированных государственных учреждений (предприятий) или частных экспертных фирм. Существенным моментом является международная практика. Так, например, западноевропейские фирмы-производители оборудования для банковских СЗ придерживаются следующих критериев оценки угроз, согласно которым для сейфовых комнат-хранилищ ценностей и компьютерной информации определены следующие приоритеты:

- защита от чрезвычайных обстоятельств (пожары, аварии, стихийные бедствия, терроризм и т.п.);

- несанкционированное проникновение в сейфовую комнату (кража ценностей или информации).

Однако для операционных залов распределение критериев другое:

- защита от несанкционированной записи или считывания информации;

- защита от чрезвычайных обстоятельств.

Данный подход позволяет дифференцировано и оптимально подойти к распределению ресурса, выделенного для СЗ.

1.3. Подход к созданию концепции зашиты

В основе разработки различных СЗ и организации ее функционирования лежит принцип создания замкнутых, последовательных, начинающихся за пределами контролируемой зоны и концентрически стягивающихся к особо важным выделенным помещениям рубежей (рис. 2.).

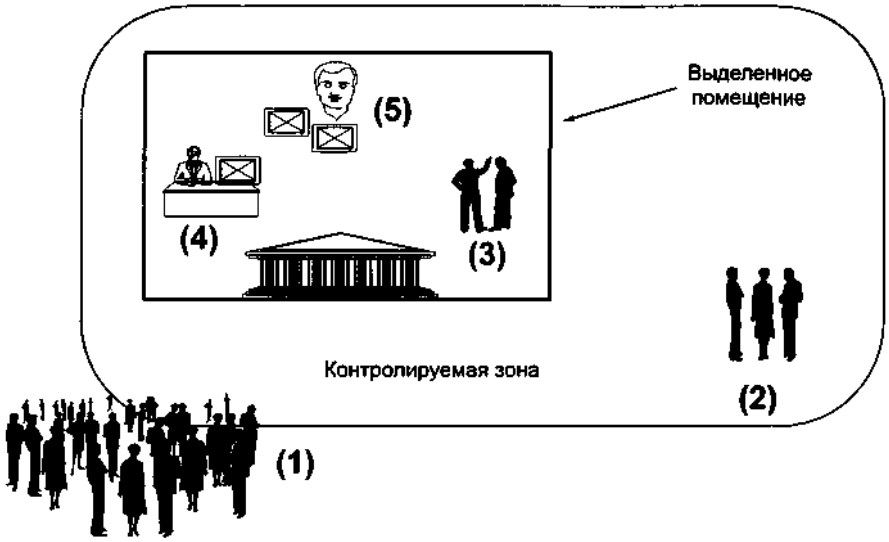


Рис. 2 Рубежная модель СЗИ (в скобках указаны рубежи защиты)

На каждом рубеже угрозы нарушению безопасности должны быть обнаружены и по возможности ликвидированы, а в случае невозможности ликвидации, их распространению должны препятствовать последующие рубежи. Основу планирования и оборудования контролируемых зон (организованных рубежами) составляют принципы равномощности и комплексности.

Использование рубежной СЗ обусловлено тем, что она позволяет обеспечить безопасность: при наличии широкого спектра разнородных угроз (от терроризма до изощренных попыток проникновения в вычислительную систему банка); при использовании различных технологий обработки информации путем глобального контроля; за счет оптимального распределения ресурсов СЗ с учетом приоритета угрозы.

Следует отметить, что чем сложнее защита каждого рубежа, тем больше времени потребуется ЗЛ для его преодоления и тем вероятнее его обнаружение. Из этого следует, что защита каждого рубежа должна взаимно дополнять друг друга и эффективность всей СЗ будет оцениваться как минимальное время, которое ЗЛ должен затратить на преодоление всех ее рубежей. За это время (безопасное время) он должен быть обнаружен и обезопасен сотрудниками СБ.

1.4. Классификация ЗЛ

Ранее было показано, что при наличии преднамеренных угроз их источником в конечном счете является человек. Нарушение безопасности коммерческой деятельности банка зависит от целей, возможностей и уровня подготовки ЗЛ. Поэтому

классифицировать ЗЛ можно исходя из:

- неопределенности процесса защиты, вызванной наличием человеческого фактора;

- рубежной СЗ;

- возможности ЗЛ повлиять на коммерческую деятельность банка.

При сочетании этих принципов возможна следующая классификация ЗЛ (см. рис. 2. и рис. 3.):

1) ЗЛ находится за пределами контролируемой зоны;

2) ЗЛ находится в пределах контролируемой зоны, но без доступа в выделенные помещения;

3) ЗЛ имеет доступ в выделенные помещения и работает в них;

4) ЗЛ - сотрудник банка, имеет доступ в выделенные помещения и работает в них;

5) ЗЛ - сотрудник СБ.

Резюмируя, можно сказать, что, зная возможные угрозы, виды ЗЛ, можно предположить, каким образом каждый вид ЗЛ может нарушить безопасность объектов защиты на том или ином ее рубеже. Это позволяет дифференцировано подходить к комплексу средств и методов защиты, определяя необходимые мероприятия и средства защиты применительно для каждого вида ЗЛ.

1.5. Структура Службы безопасности

Уточнив основные элементы процесса защиты (объекты защиты, виды ЗЛ и их потенциальные возможности, определенные рубежами защиты), мы можем определить их взаимное соответствие. Для этого нам необходимо объединить два основных понятия: объект защиты и ЗЛ во всех их формах отношений.

Полное множество отношений для всех объектов защиты и форм атак ЗЛ на них можно представить в виде таблицы, где строками являются объекты защиты, а столбцами - виды ЗЛ (рис. 3.).

Данная таблица следует из принципа "защита тотальная". Она однозначно показывает необходимость дифференцированного подхода к созданию мероприятий безопасности для каждого вида ЗЛ, объектов защиты и их последующую комплексную увязку.

Исторически уже сложилась мировая практика обеспечения безопасности объектов защиты как от преднамеренных, так и не преднамеренных угроз безопасности. Она определяет взаимосвязь объектов защиты с возможной формой ЗЛ и среду, в которой он осуществляет свои злоумышленные действия. Любая среда обладает специфическими особенностями, которые характерны для конкретного направления защиты, из которых следует структура функциональных подразделений СБ:

- группа режима;

- служба охраны;

- пожарная охрана;

- аналитическая группа;

- детективная группа;

- группа комплексного контроля ЗИ;

- группа защиты от НСД;

- криптографическая группа.

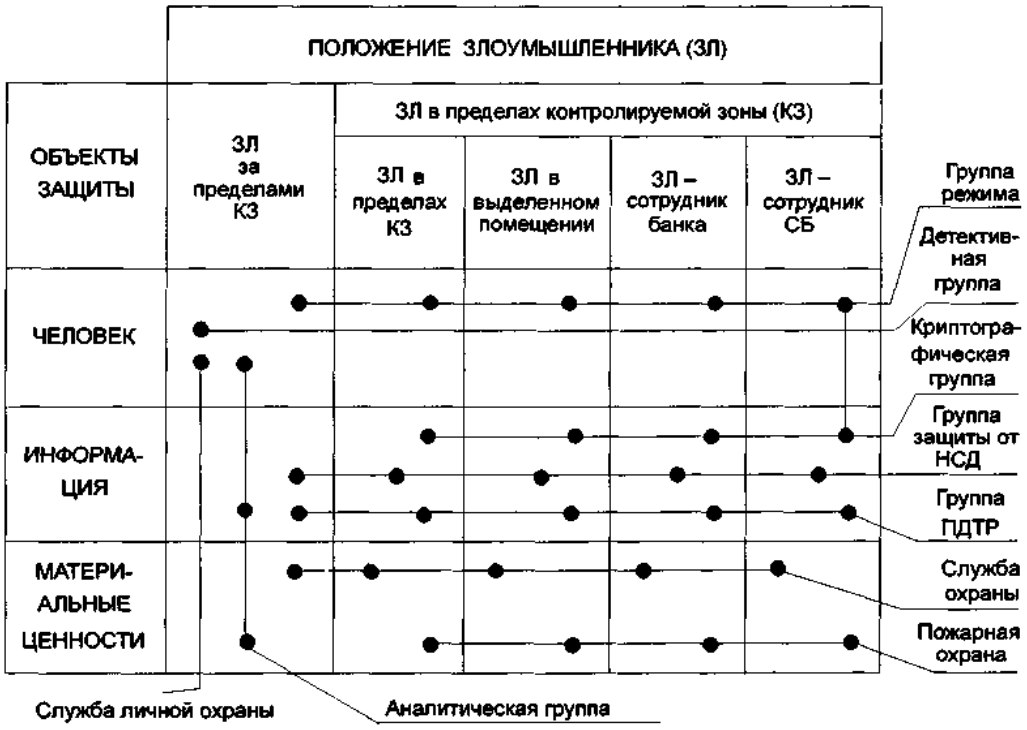


Рис. 3 Взаимодействие объектов защиты с видами ЗЛ, их возможностями и традиционно сложившимися службами

Кроме того, в СБ для ее успешной деятельности необходимы вспомогательные подразделения:

- группа консультантов по различным вопросам деятельности СБ;

- юридическая служба (например, юрист-консультант по безопасности в составе юридической группы банка).

Функциональная структура СБ банка показана на рис. 4.

Численный состав СБ и их отдельных групп определяется производственной необходимостью и объемом финансирования.

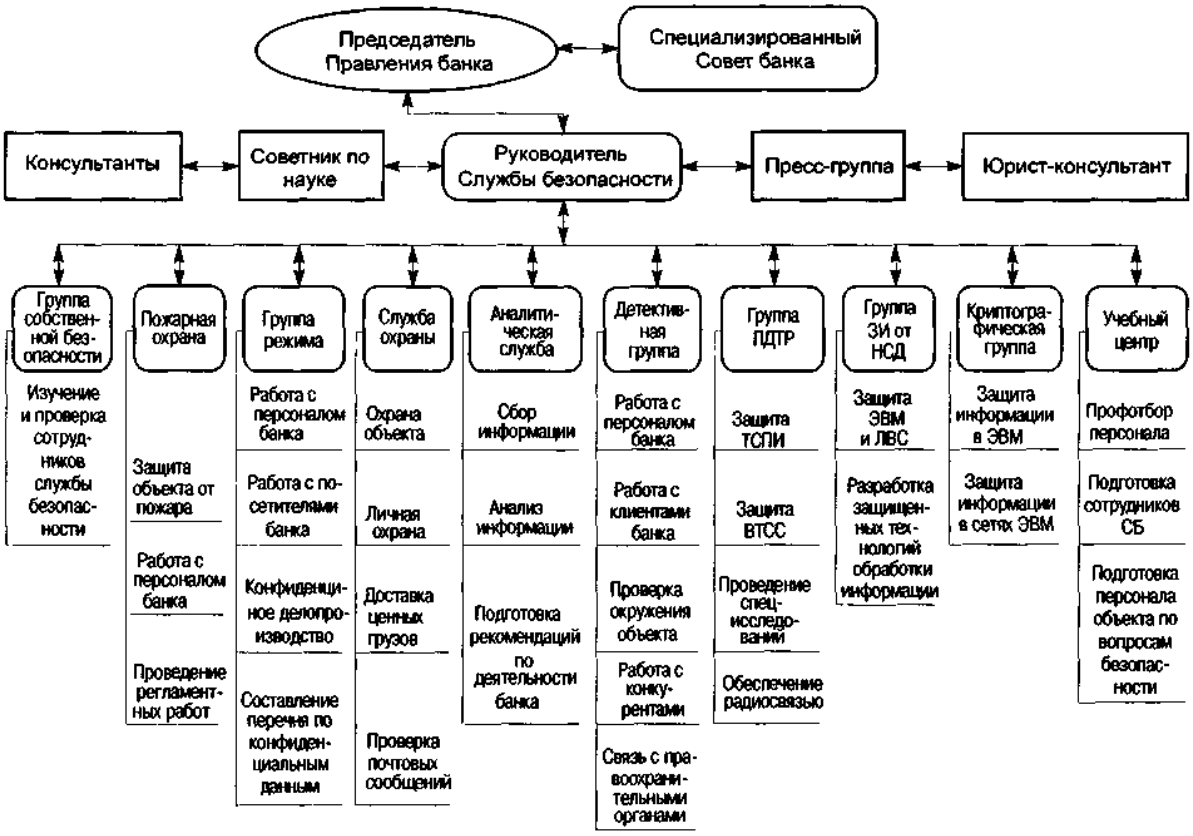


Рис.4. Примерная структура и функции Службы безопасности банка

Вопрос 2. ПРАВОВЫЕ ОСНОВЫ ДЕЯТЕЛЬНОСТИ СБ

Основные положения, состав и организация СБ имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах банка и руководствуются Положением о СБ банка.

В основу деятельности СБ должны быть положены:

1) Гражданский кодекс Российской Федерации (часть I и II);

2) Закон Российской Федерации "О банках и банковской деятельности";

3) Закон Российской Федерации "О государственной тайне";

4) Закон Российской Федерации "О приватизации государственных и муниципальных предприятий РСФСР";

5) Закон Российской Федерации "О конкуренции и ограничении монополистической деятельности на товарных рынках";

6) Закон Российской Федерации "О безопасности";

7) Закон Российской Федерации "Об информации, информатизации и защите информации";

8) Уголовный кодекс Российской Федерации;

9) Постановление Правительства РФ от 05.12.1991 г. № 35 "О перечне сведений, которые не могут составлять коммерческую тайну";

10) Закон Российской Федерации "О частной детективной и охранной деятельности в Российской Федерации";

11) Федеральный закон "Об оперативно-розыскной деятельности в Российской Федерации";

12) Закон Российской Федерации "Об оружии";

13) Кодекс законов о труде;

14) Устав банка, коллективный договор, трудовые договора, правила внутреннего распорядка, технологические руководства и инструкции банка, должностные функции и обязанности руководителей, специалистов, рабочих и служащих.

Организационно СБ должна подчиняться собранию учредителей и акционеров банка, а в текущей деятельности - Председателю Правления.

Состав и функции структурных подразделений СБ определяются По-ложением о СБ. На основе Положения составляется штатное расписание СБ, определяется степень ответственности за выполнение возложенных на нее задач. Руководителем СБ назначается ответственное лицо в ранге заместителя Председателя Правления банка, отвечающее персонально за все вопросы безопасности банка.

Права, обязанности и ответственность сотрудников СБ.

Сотрудники СБ в целях безопасной деятельности банка имеют право:

- требовать от всех сотрудников и клиентов банка строгого и неукоснительного выполнения пропускного, внутриобъектового режима, правил трудового распорядка, нормативных и договорных обязательств по безопасности действующих в банке;

- требовать от руководителей подразделений и исполнителей правильного и своевременного выполнения нормативных документов по организации и ведению специального делопроизводства;

- проводить тотальные проверки эффективности защиты ресурсов, информации, помещений и объектов банка;

- запрещать использование технических и программных средств, не соответствующих требованиям безопасности;

- требовать от функциональных подразделений необходимые сведения для анализа информационной безопасности;

- вносить предложения по совершенствованию правовых организационных и инженерно-технических мероприятий по коммерческой безопасности;

- планировать деятельность СБ, утверждая планы работы у Председателя Правления банка;

- требовать гарантированного финансового обеспечения мероприятий, предусмотренных планом работы СБ.

Сотрудники СБ обязаны:

- разрабатывать организационные, организационно-технические и технические мероприятия по обеспечению надежной безопасности деятельности банка;

- осуществлять постоянный контроль за соблюдением требований по безопасности банка;

- постоянно контролировать работоспособность СЗ;

- обеспечивать проведение специсследований технических и программных средств и аттестацию выделенных помещений;

- участвовать в акции восстановления и организации функционирова-ния банка в случае чрезвычайных ситуаций;

- осуществлять сбор и анализ информации для выявления злоумыш-ленных действий;

- докладывать руководству о фактах нарушения требований нормативных документов и других действиях, могущих привести к нарушению коммерческой безопасности банка;

- отчитываться перед руководством СБ о состоянии СЗ и планах своей деятельности;

- организовывать и проводить обучение сотрудников банка выполнению требований безопасности.

Сотрудники несут персональную ответственность за личное нарушение мер безопасности, за неудовлетворительное исполнение служебных обязанностей, а также за неиспользование своих прав при исполнении своих функциональных задач.

Вопрос 3. ФУНКЦИИ, ЗАДАЧИ И ОСОБЕННОСТИ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ БЕЗОПАСНОСТИ

3.1. Общие положения

Исходя из возможных угроз по всем видам безопасности можно утверждать, что деятельность СБ весьма разнообразна: от работы по обеспечению безопасности персонала до решения чисто технических вопросов, включающих в себя проверку и аттестацию технических и программных средств на соответствие специальным требованиям. Поэтому основными функциями деятельности СБ являются:

- определение целей и приоритетных направлений работы по обеспечению всех видов безопасности деятельности банка;

- разработка проектов защиты для каждого вида безопасности, их реализация, приемка и контроль за поддержанием в постоянной работоспособности;

- разработка нормативных документов для всех видов безопасности с учетом степени конфиденциальности и контроль за их соблюдением всеми сотрудниками и клиентами банка;

- организация обучения персонала правилам соблюдения и поддержания безопасности деятельности;

- организация и проведение совместно с другими подразделениями банка специальных мероприятий в отношении конкурирующих банков и других организаций;

- взаимодействие с правоохранительными органами по вопросам безопасности.

Отметим теперь специфические особенности в работе СБ, которые являются следствием принципов, сформулированных в главе 1.

Первая особенность. В принципе можно создать абсолютно надежную СЗ. Однако ее стоимость будет значительной. Вполне естественным ограничением собственности СЗ является стоимость объектов защиты. Это верхний предел затрат на СЗ. Для того, чтобы СЗ не требовала существенного расхода финансовых средств банка, приходится использовать не абсолютные средства и методы СЗ, т.е. подвергать себя риску нарушения безопасности. Без определенной степени риска деятельность любого банка просто неосуществима Таким образом, стоимость защищаемых объектов и первоначальное вложение капитала в средства и методы безопасности определяют степень риска нарушения безопасности.

Вопрос о том, какова должна быть величина риска, определяется средствами от прибыли банка, вложенными на поддержание СЗ. Опять-таки для существования банка последний может тратить на содержание СЗ только часть своей прибыли, которая и определяет величину риска Вопрос о количественной степени риска, зависящей от стоимости объектов защиты и части прибыли банка, отпущенной на поддержание СЗ, в настоящее время является открытым, хотя существуют различные подходы к его решению. Однако, как показал их анализ, они, как правило, эмпирические и во многом зависят от конкретных условий.

Вторая особенность. Рано или поздно нарушение любого из видов безопасности будет известно. Возникает вопрос: как предупредить нарушение безопасности или хотя бы минимизировать это время? В первом случае ущерб будет предотвращен, а во втором, как правило, будет минимален.

Все возможные нарушения безопасности возникают в конечном счете из-за риска, обусловленного недостаточностью средств на создание СЗ. Недостаточность средств влечет за собой возникновение нештатных ситуаций, которыми и пользуется ЗЛ. Возникновение нештатных ситуаций обусловлено неопределенностью процесса защиты, т.е. неизвестно, в какое время, где будут происходить злоумышленные действия, каким образом и при каких условиях они могут возникнуть.

Практическим методом уменьшения риска является выполнение глобального контроля за действиями всех сотрудников и клиентов банка, их регистрации и последующего анализа. В первом случае, при идеальном контроле, злоумышленные действия будут предупреждены. Однако идеальный контроль опять-таки невозможен, и поэтому нельзя говорить об абсолютной защите. Во втором случае регистрация всех действий и последующий за ней анализ позволяет минимизировать время неопределенности нарушения безопасности. Однако, аналогично контролю, нельзя осуществить абсолютную регистрацию и ее анализ.

Таким образом, на действия потенциального ЗЛ влияют следующие возложенные на СБ функции:

- предупреждение;

- контроль за текущей ситуацией;

- регистрация;

- анализ результатов регистрации.

Предупреждение является активным сдерживающим фактором и должно использоваться всеми подразделениями СБ. Следует отметить, что чем раньше придет сигнал предупреждения, тем больше имеется времени у сотрудников СБ принять решение для блокирования злоумышленных действий.

Формы предупреждения могут быть самыми различными, но, разрабатывая систему безопасности, виды предупреждения должны быть максимально полными, чтобы даже учитывать психологию ЗЛ, убеждая его в том, что нет необходимости предпринимать какие-либо попытки, т.к. они потерпят неудачу.

Контроль и регистрация действий потенциальных ЗЛ в текущей ситуации необходимы в любом случае, т.к. никогда не может быть уверенности, что меры предупреждения являются гарантией безопасности и, следовательно, нападение возможно в любой момент времени. Контроль и регистрация текущего состояния атмосферы безопасности должны быть максимально всеобъемлющими и информативными.

Анализ по результатам регистрации эффективности принятых мероприятий является важным этапом в обеспечении безопасности, т.к. окружающая среда и, вполне естественно, действия ЗЛ не являются статическими, а эволюционируют по принципу - выживает сильнейший. Составляющие фактора времени показаны на рис. 5.

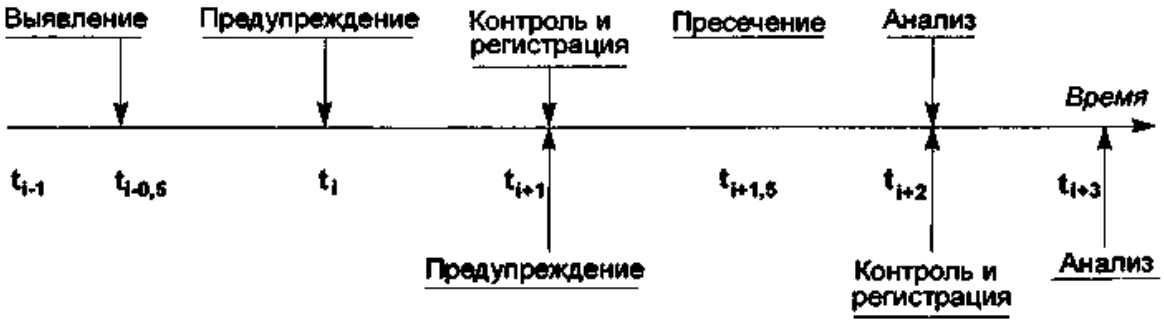


Рис. 5 Распределение функций защиты во времени

Следует особо отметить, что самые совершенные средства и методы сохранения безопасности не могут сами обеспечить должной безопасности, если не работает человеческий фактор - дисциплинированность, умение и ответственность персонала. Таким образом, проблема безопасности может быть решена лишь в том случае, если все сотрудники банка объединят свои усилия.

Резюмируя вышесказанное, можно сделать следующие выводы:

1. СЗ никогда не следует рассматривать как абсолютно надежную, всегда существует определенная степень риска.

2. Для того чтобы ущерб был минимальным, СЗ должна быть макси-мально всеобъемлющей.

3. Существенную роль в минимизации ущерба играет фактор времени обнаружения злоумышленных действий.

4. Эффективность действия СЗ в конечном счете зависит от человека (человеческий фактор).

Рассмотрев общие положения, перейдем к особенностям и основным функциям деятельности подразделений СБ. Несмотря на то, что проблема обеспечения безопасности имеет комплексный характер и каждое подразделение СБ участвует в работе других подразделений, следует выделить основные объекты защиты для каждого подразделения. Соответствие подразделений СБ их основным объектам защиты показано на рис. 6.

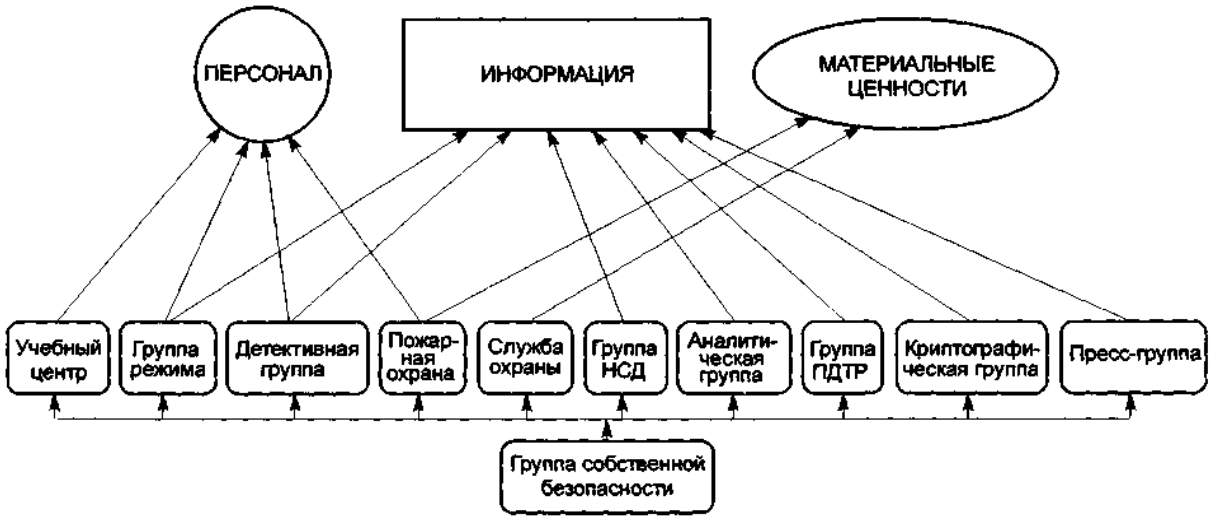


Рис. 6. Соответствие подразделений СБ их основным объектам защиты

3.2. Группа режима

Группа режима является самостоятельным подразделением СБ и подчиняется начальнику СБ. В своей деятельности она руководствуется требованиями "Инструкции по режиму и охране". Главными функциями группы режима являются:

- организация пропускного и внутриобъектового режима;

- участие в разработке "Перечня сведений, составляющих коммерческую (банковскую) тайну";

- организация и ведение конфиденциального делопроизводства;

- разработка положения и инструкций о порядке работы со служебной информацией и сведениями, составляющими государственную или коммерческую тайну;

- разработка разрешительной системы и обеспечение допуска к сведениям,

составляющим служебную и коммерческую (банковскую) тайну;

- разработка нормативов и проверка их выполнения сотрудниками банка, работающими с информацией различной категории конфиденциальности;

- контроль соблюдения режима доступа к сведениям и документам;

- ведение учета пользования, хранения и размножения материалов, составляющих государственную или коммерческую (банковскую) тайну;

- контроль за порядком засекречивания и рассекречивания документов;

- периодический контроль выходящих за пределы банка документов и материалов на наличие служебных и конфиденциальных сведений;

- уничтожение документов, материалов, машинных носителей, которые могут способствовать раскрытию государственной или коммерческой тайны или технологий их обработки;

- аттестация и периодический контроль (совместно с другими подразделениями СБ) технологических процессов обработки информации;

- организация и проведение изучения кандидатов для приема на работу;

- периодические проверки сотрудников банка на выявление степени их лояльности;

- повышение квалификации сотрудников банка, работающих с документами различной степени конфиденциальности;

- работа с сотрудниками банка, связанных со сторонними организациями и клиентами банка по сохранению коммерческой безопасности банка.

Резюмируя вышесказанное, можно отметить, что

-лавным объектом деятельности группы режима являются сотрудники объекта, а целью - создание внутренней атмосферы объекта защиты.

3.3. Служба охраны

Служба охраны является самостоятельным структурным подразделением СБ и тесно взаимодействует с группой режима. В своей деятельности она руководствуется требованиями "Инструкции по организации режима и охраны". Численность группы охраны определяется конкретной криминогенной обстановкой. В случае экстремальных ситуаций возможно привлечение специалистов сторонних организаций только для решения конкретных ограниченных задач.

Деятельность службы охраны должна осуществляться в трех направлениях:

1. Охрана объектов банка.

2. Охрана ценных грузов при их перевозке.

3 Обеспечение личной безопасности руководства и сотрудников банка.

Деятельность подгруппы охраны объектов банка традиционна и направлена в основном на обеспечение пропускного и внутриобъектового режима. Для ее функционирования она оснащается средствами охранно-пожарной сигнализации (ОПС).

Подгруппа сопровождения ценных грузов, хотя и входит в группу охраны, подчиняется непосредственно начальнику СБ. Ее деятельность регламентируется внутриведомственными документами и специальными положениями. Учитывая особые условия работы данной подгруппы, она должна комплектоваться из числа высококвалифицированных профессионалов, оснащенных спецтранспортом и средствами связи и состоять исключительно из штатных сотрудников банка. Численность и состав подгруппы определяется производственной необходимостью.

Подгруппа обеспечения личной безопасности руководства и сотрудников банка в своей деятельности руководствуется документами, регламентирующими охранную деятельность и специальным Положением, разрабатываемым СБ с учетом конфетной обстановки. Основными задачами подгруппы являются: охрана руководства банка в обычных и экстремальных условиях; проведение учебы по направлениям соблюдения личной безопасности и поведения в экстремальных условиях; поддерживание контактов с правоохранительными органами и СБ других организаций.

Количественный состав службы и привлечение сторонних организаций, занимающихся охранной деятельностью, определяется руководителем СБ в соответствии с обстановкой.

3.4. Пожарная охрана

Зарубежные специалисты СБ банков неоднократно подчеркивают, что одновременную угрозу всем объектам защиты банковской деятельности наиболее часто представляют пожары в помещениях банка. При этом даже незначительное возгорание может привести к потере огромного объема информации, что обусловлено сильной уязвимостью информации, обрабатываемой средствами вычислительной техники. Поэтому, вполне естественно, в структуре СБ должна присутствовать группа пожарной охраны.

Пожарная охрана является самостоятельным подразделением СБ. Деятельность группы регламентируется "Положением о государственном пожарном надзоре", "Наставлением по организации работы органов государственного пожарного надзора", "Сборником правил пожарной безопасности" и внутренними документами банка.

Главной задачей группы пожарной охраны является создание противопожарной обстановки на основе работы с персоналом банка, использования средств пожарной сигнализации и пожаротушения; работы с органами гостехнадзора, госэнергонадзора, пожарно-техническими комиссиями и пожарными службами организаций ближайшего окружения банка.

3.5. Аналитическая группа

Наличие недобросовестной конкуренции возможных злоумышленных действий со стороны клиентов и конкурентов банка требует активного противодействия. Оно возможно только в том случае, если СБ располагает о них информацией. Сбором, анализом и оценкой степени опасности деятельности банка и занимается аналитическая группа. Таким образом, главной целью деятельности аналитической группы является создание благоприятной атмосферы безопасности банка, которая состоит из двух слагаемых:

1. Сведение возможных негативных действий клиентов и конкурентов банка до минимума.

2. Максимизация эффективности своих действий относительно клиентов и конкурентов банка.

Другими словами, целью работы аналитической группы является обеспечение информационной безопасности банка.

Принципиальное отличие в работе аналитической группы от работы других подразделений СБ заключается в том, что она, в общем случае, должна работать на перспективу, т.е. прогнозировать возможные события, оценивая возможную прибыль или ущерб, и своими прогнозами, в конечном счете, приносит прибыль банку, которая проявляется в неявном виде.

Аналитическая группа является самостоятельным подразделением СБ и подчиняется ее руководителю. Она организует свою деятельность в тесном взаимодействии со всеми структурными подразделениями банка. Численный состав группы определяется руководителем СБ в зависимости от конкретной ситуации. При этом допускается привлечение специалистов сторонних организаций.

3.6. Детективная группа

Детективная группа является самостоятельным подразделением СБ и подчиняется непосредственно руководителю СБ. В своей деятельности детективная группа руководствуется Законом "О частной детективной и охранной деятельности в Российской Федерации" и Положением о СБ. Детективная группа:

- разрабатывает и проводит специальные мероприятия по наблюдению за отдельными сотрудниками и клиентами банка, а также жителями ближайшего к банку окружения, в действиях которых содержатся угрозы безопасности деятельности банка;

- осуществляет совместно с группой режима проверку кандидатов для приема на работу в банк;

- по заданию группы режима проводит контроль лояльности сотрудников банка;

- поддерживает контакты с правоохранительными органами по всем вопросам, связанным с угрозами безопасности деятельности банка;

- содействует обеспечению возврата просроченных кредитов;

- совместно с аналитической группой проводит специальные мероприятия по отношению к организациям-клиентам банка и конкурентам банка.

Количественный состав детективной группы определяется производственной необходимостью. Для выполнения ряда заданий допускается привлечение специалистов сторонних организаций.

3.7. Группа ПДТР

Группа ПДТР является самостоятельным подразделением СБ и подчиняется руководителю СБ. В своей деятельности группа ПДТР руководствуется нормативными документами по ЗИ.

Данное направление в ЗИ характеризуется тем, что ЗЛ для получения информации использует самые разнообразные технические средства, начиная с традиционно визуального наблюдения за деятельностью банка и заканчивая проникновением в помещение банка с целью установки закладных устройств.

Отличительной особенностью данного направления является то, что защищаемая информация имеет, как правило, кроме основной среды передачи информации еще несколько побочных сред. Поясним это на примере. Пусть два сотрудника банка, находясь в выделенном помещении, ведут деловой разговор. Для них основной средой передачи информации является воздушное пространство. Предположим, что ЗЛ находится в пределах видимости, но за пределами контролируемой зоны. Тогда он может получить информацию с помощью направленных микрофонов, визуального наблюдения артикуляции губ разговаривающих сотрудников, с помощью лазерного съема информации со стекол окон банка, за которыми происходит разговор, и возможно с использованием радиозакладок. Наличие нескольких сред основного сигнала показано на рис. 7.

Из приведенного примера следует, что информация может иметь несколько различных форм представления и для каждой ее формы существует не одна, а несколько сред ее существования. Следовательно, основная цель ПДТР состоит в том, чтобы контролировать и блокировать весь спектр колебаний, начиная от единиц герц и заканчивая рентгеновским излучением. Таким образом, общая постановка данного направления ЗИ может быть представлена схемой:

Источник информации → Среда → Сигнал → Приемник ЗЛ

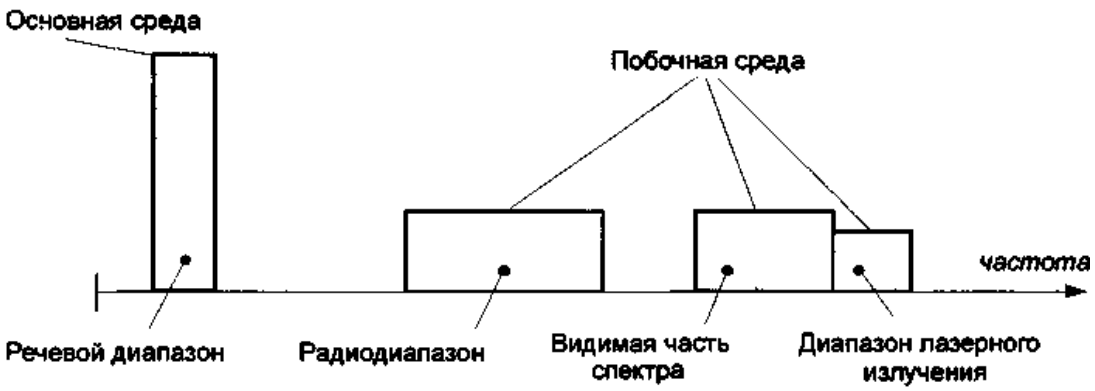


Рис. 7. Среды опасного сигнала

Исходя из представленной схемы определяются задачи группы ПДТР и возникает методология ЗИ от технических средств разведки, которая включает в себя следующие ключевые моменты:

1. Определение источников информации.

2. Определение сред, где может существовать информация.

3. Определение опасных сигналов в выявленных средах.

4. Измерение величины опасного сигнала.

5. Уменьшение величины или скрытие (зашумление) опасного сигнала в соответствии с нормативными документами.

3.8. Группа зашиты информации от НСД

Группа защиты информации от НСД в ЭВМ является самостоятельным структурным подразделением СБ и подчиняется начальнику СБ. Целью деятельности группы НСД является защита информации, обрабатываемой в ЭВМ и передаваемой по линиям связи. В своей деятельности группа НСД руководствуется нормативными документами, национальными и международными стандартами по обработке и ЗИ. В целях экономии средств на разработку программного обеспечения и систем защиты допускается привлечение специалистов сторонних организаций.

Блокирование НСД к информации в ЭВМ является в настоящее время весьма актуальной и сложной задачей. Это обусловлено различными причинами, к которым в первую очередь следует отнести: невозможность без ЭВМ эффективной работы банка; реализацию сложных сетевых режимов работы; присутствие человеческого фактора.

Угрозы НСД носят алгоритмический характер, многие задачи которого не решены в настоящее время. Сформулируем основные проблемы данного направления. Это в первую очередь система разграничения доступа. Данная проблема предусматривает отсутствие возможности как несанкционированного считывания, так и несанкционированной записи информации. В противном случае будет нанесен ущерб законному владельцу информации (нарушение безопасности информации). Сложность данной проблемы заключается в том, что ПЭВМ разрабатывается из предрасположенности к ее пользователю, а вопросы ЗИ считаются второстепенными, т.к. они ограничивают возможности пользователей.

Системы разграничения доступа обычно базируются на моделях матричного типа и реализуются в виде специальных компонент операционных систем или систем управления базами данных. Однако они имеют существенный недостаток - необходимость детального описания прав каждого пользователя для каждой технологической ситуации, что делает их достаточно громоздкими.

Для преодоления указанного недостатка используют иерархические или многоуровневые модели защиты, которые используют концепцию ядра безопасности. При этом создание ядра безопасности как изолированной совокупности программно-аппаратных средств имеет тот недостаток, что необходимо доказать корректность его

функционирования, а также появляется проблема полной формальной верификации.

В обоих случаях на безопасность информации существенно влияет человеческий фактор. Данное обстоятельство обусловлено тем, что децентрализация доступа к разнородным информационным объектам, а также отсутствие эффективных средств изоляции программ и данных позволяет взломщикам (хакерам) получить доступ к защищаемой информации.

Вторая проблема НСД, тесно примыкающая к первой, это проблема создания надежных протоколов обмена информацией как между пользователями, так и во время работы всего вычислительного процесса. В настоящее время основные черты ее решения уже наметились как в вопросах стандартизации работы средств вычислительной техники, так и при использовании криптографических средств.

Третья проблема данного направления, объединяющая первые две, это проблема создания защищенных информационных технологий. Она является комплексной с функциональной и алгоритмической точек зрения. Отметим только, что проблема компьютерного вируса, так нашумевшая несколько лет назад, относительно просто решается в рамках защищенных информационных технологий путем соблюдения организационных, алгоритмических и профилактических мероприятий.

Резюмируя, можно сказать, что создание защищенных информационных технологий (создание защищенной программной среды) является главной задачей группы защиты информации от НСД.

3.9. Криптографическая группа

Криптографическая группа является структурным подразделением СБ. В своей работе она руководствуется нормативными документами Гостехкомиссии РФ и "Инструкцией по обеспечению криптографической защиты банка".

Целью деятельности криптографической группы является обеспечение защиты информации при передаче ее по каналам связи. Основными задачами криптографической службы являются:

1) обеспечение аттестованными аппаратными и программными средствами криптографической защиты;

2) выработка ключей для пользователей;

3) инструктаж и контроль за работой пользователей при работе со средствами криптографической защиты;

4) проверка функционирования и ремонт средств криптографической защиты.

Криптографическая группа должна состоять только из штатных сотрудников банка. Ее состав и численность определяется производственной необходимостью.

3.10. Учебный центр

Учебный центр (УЦ) является самостоятельным структурным подразделением СБ. В УЦ

с помощью как штатного, так и привлеченного профессорско-преподавательского состава осуществляется подготовка и переподготовка сотрудников СБ и персонала объекта по различным спектрам проблемы обеспечения безопасности. Содержание и объем подготовки должны иметь теоретическую и прикладную направленность на основе соблюдения принципов оптимального сочетания фундаментализации и профессионализации обучения.

Основной учебной специализацией являются должностные обязанности сотрудников СБ и объекта. Учебные программы должны предусматривать формирование базовых основ правовых знаний по вопросам безопасности, психологическую, физическую, специальную, медицинскую, огневую, техническую подготовку.

Процесс обучения и переподготовки должен носить комплексный характер, обеспечивающий гармоничное сочетание учебной, научной и воспитательной работы, направленной на достижение высокого профессионализма слушателей.

Базовое обучение и подготовку желательно осуществлять по модуль-ной схеме с учетом конкретных требований к профессиональным качествам каждого из обучаемых.

В структуре УЦ необходимо иметь специальное подразделение, предназначенное для решения задач определения на основе современных психофизиологических и иных методик профессиональной пригодности кандидатов для замещения вакантных должностей на объекте и его СБ.

3.11. Пресс-группа

Пресс-группа осуществляет функции по проведению целевых пропа-гандистских акций в интересах создания благоприятной для объекта защиты обстановки в конкурентной и партнерской среде, определяет объем информации об объекте, передаваемый в средства массовой информации, организует пресс-конференции и брифинги для российских и зарубежных корреспондентов, поддерживает деловые и неформальные отношения с источниками в СМИ. Важное место занимает анализ отечественной и иностранной прессы об объекте.

3.12. Группа собственной безопасности

Группа собственной безопасности (ГСБ) является структурным подразделением СБ, подчиненным непосредственно первому руководителю службы безопасности объекта. ГСБ обеспечивает безопасность деятельности СБ объекта, защиту ее сотрудников, осуществляет комплексные мероприятия по предупреждению, выявлению и пресечению фактов противоправной деятельности со стороны сотрудников СБ, разрабатывает меры по защите информации и служебной тайны о службе безопасности объекта.

Вывод: мы рассмотрели концепцию и структуру СЗ банка на основе принципов мировой практики защиты. Однако, как подчеркивалось во введении, обеспечение безопасности для каждого конкретного случая является сугубо индивидуальным, т.к. имеются специфические особенности каждого объекта защиты. Выявление этих

особенностей является сложной задачей, как при разработке конкретной концепции, так и построения и эксплуатации СЗ. Здесь необходима помощь опытных специалистов.

Это объясняется тем, что любое нарушение безопасности обусловлено тремя основными причинами:

1) недооценкой степени риска;

2) наличием нештатных ситуаций, которыми может воспользоваться ЗЛ (стандартность мышления разработчиков СЗ);

3) неблагоприятными внешними или внутренними условиями, а также их создание ЗЛ для инициации нештатных ситуаций.

Общая концепция безопасности банка позволяет строить отдельную концепцию для каждого направления защиты. Последующие главы детально раскрывают задачи и особенности работы каждой группы СБ.

ЛЕКЦИЯ 5
ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ

Учебные вопросы:

1. Правовое регулирование и организация работ по защите информации.

2. Руководящие нормативно-технические, методические и организационные документы в области информационной безопасности.

3. Организационные мероприятия и процедуры по обеспечению защиты информации в автоматизированных системах

Вопрос 1. ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Вопросы развития и внедрения безопасных информационных технологий тесным образом связаны не только с решением научно-технических проблем, но и с вопросами правового регулирования общественных отношений в процессе информатизации. При этом их решение в большой степени зависит не только от уровня развития вычислительной техники, но и от признания за информацией статуса товара, продукта общественного производства. Установление в законодательном порядке права собственности на информацию является важнейшим аспектом формирования информационной политики государства.

Разработка и внедрение законодательной базы информатизации невозможны без активной государственной информационной политики, направленной на построение по единому замыслу организационно-правового механизма управления информационными процессами, увязанного с научно-технической программой информатизации.

Серьезным шагом в направлении создания правовых норм, закрепляющих права и обязанности граждан, коллективов и государства на информацию, является принятие Закона РФ "Об информации, информатизации и защите информации"[3]. В указанном законе определен правовой режим информации, правила, процедуры и распределение ответственности в области защиты информации в системах ее обработки, установлен порядок правовой защиты и гарантии реализации прав и ответственности субъектов информационных взаимоотношений.

В области информатизации закон разработан как базовый по признакам охвата важнейших направлений и условий, закрепления правовых институтов и форм отношений, имеющих значение для дальнейшего развития законодательства, разработки подзаконных актов и организационных структур в этой области.

Наиболее существенными с рассматриваемых позиций в законе являются:

- статья, устанавливающая общий правовой режим информации, в которой определено отношение к информации как к возможному объекту собственности граждан, коллективов, государства и общества в целом (общественное достояние), а также как к возможному объекту пользования, с учетом деления информации на категории открытого и ограниченного доступа;

- статья, закрепляющая за собственником информации права на действия по отношению к ней и признающая за информацией статуса имущества юридических лиц;

- статья, декларирующая право собственности на программно-информационную продукцию наряду с авторскими правами;

- статья, определяющая режим доступа к информации.

Глава 4 закона полностью посвящена вопросам защиты информации и информационных систем, причем подчеркивается, что защита информации в системах ее обработки направлена на обеспечение важнейших конституционных прав личности, коллектива и государства, на охрану прав собственности, обеспечения безопасности населения, безопасности и обороноспособности страны. Физическим и юридическим лицам предоставлено право на защиту информации и систем ее обработки от преступных посягательств, несанкционированных действий и других видов угроз.

В статье 20 провозглашены цели защиты информации и систем ее обработки, статья 15 определяет требования к владельцу информационной системы по обеспечению уровня защиты информации в соответствии с правилами, установленными собственником информации, а статья 19 предусматривает создание государственной системы сертификации продукции по требованиям безопасности информации и лицензирования деятельности предприятий по оказанию услуг в области защиты информации.

Весьма важной с точки зрения осуществления права на информацию, защиту прав субъектов отношений в области информатизации является глава 3, в которой для физических и юридических лиц, являющихся участниками информационных отношений, гарантируются такие виды юридической защиты, как судебная защита, страхование интересов собственника, обеспечение возмещения ущерба, оказание юридической помощи и т.п.

Вопросы ответственности за нарушения и посягательства на информацию и информационные системы должны быть предусмотрены в уголовном и гражданском законодательстве. Однако ни в одном из уголовных кодексов бывших союзных республик нет статей, специально посвященных компьютерным преступлениям. Нет таких определений и в гражданском законодательстве и в нормах административного права об ответственности за нарушения в сфере использования средств вычислительной техники. Только в уголовном законе может быть определено, что именно является преступлением, то есть деянием, запрещаемым под страхом наказания. В законодательстве об административных правонарушениях устанавливаются нормы ответственности за правонарушения, не повлекшие общественно опасных последствий.

Действующее уголовное законодательство при небольшой корректировке может быть использовано при квалификации некоторых компьютерных преступлений. Так, умышленное уничтожение носителей с машинной информацией, уничтожение (удаление) файлов, изменение (модификация) записей файлов может квалифицироваться по статье 98 УК РФ "Умышленное уничтожение или повреждение государственного или общественного имущества". Для того чтобы заработали уголовно-правовые и административно-правовые нормы, необходимо, чтобы законом был установлен порядок санкционированного доступа к информации в автоматизированные системы (АС).

По действующему законодательству информация сама по себе предметом хищения быть не может, однако может использоваться для совершения других преступлению, например для получения сведений, составляющих государственную тайну, и дальнейшего их разглашения (статья 75 УК РФ).

Действующие правовые нормы трактуют понятие "хищение" как изъятие информации из пользования настоящим владельцем. При несанкционированном копировании никакого изъятия из пользования не происходит. Однако и нормы, касающиеся защиты авторских прав, не всегда подходят, хотя "Основами гражданского законодательства" они распространены на программно-информационную продукцию. Для реализации авторского права на компьютерную информацию соответствующие нормы должны быть включены в гражданский кодекс. В связи с этим представляется целесообразным ввести в законодательство норму, трактующую хищение информации как уголовное преступление.

Проблема квалификации компьютерных преступлений, ее "узкие места" и возможные перспективы решения достаточно полно изложена в работах [4, 5], откуда цитируются вышеуказанные предложения.

В качестве возможного правового решения этой проблемы можно привести некоторые положения проекта Закона Российской Федерации "Об ответственности за правонарушения при работе с информацией" [6].

Отличительной особенностью этого закона с точки зрения безопасности обрабатываемой информации можно признать статью 4, определяющую следующие основания уголовной, административной или дисциплинарной ответственности за совершенные правонарушения:

- нарушение технологии обработки информации, норм и требований по ее защищенности и правил доступа к ней;

- несанкционированный доступ к информации, программным средствам или в информационную систему;

- хищение информации (как оконченное преступление или действие в составе: государственной измены, шпионажа, промышленного шпионажа, незаконного присвоения, передачи и использования коммерческой тайны);

- неправомерное искажение, модификация и уничтожение информации и программных средств, изготовление заведомо непригодного программного обеспечения;

- изготовление и распространение программ-вирусов.

Кроме того, статьи раздела 4, полностью посвященного компьютерным правонарушениям, предусматривают уровень ответственности различных групп субъектов правовых отношений за возможные нарушения норм, требований и правил, установленных по отношению к обрабатываемой информации и самим информационным системам.

Исходя из приведенных правовых актов и предложений, можно определенным образом прогнозировать состояние законодательства в области безопасное т информации при существующих тенденциях его развития.

Определенные особенности содержит в себе проблема доказательства вины правонарушителя.

Зарубежные исследования показывают, что, несмотря на успехи отдельных злоумышленников в проникновении в компьютерные системы и сети, большую опасность представляют законные пользователи этих систем и сетей, которые повинны в 80% правонарушений.

Учитывая то обстоятельство, что терминалами АС, узлами сетей и даже отдельными ПЭВМ пользуется большое количество официально допущенных к работе пользователей, задача поиска правонарушителя серьезно затрудняется. Хотя в состав программного обеспечения АС, не говоря уже о современных системах защиты информации от НСД, входят средства контроля и протоколирования действий пользователей и посторонних лиц, доказать вину конкретного субъекта, предъявляя ему в качестве улики его идентификатор или пароль, достаточно сложно по двум причинам. Во-первых, юридически очень сложно доказать, что эти атрибуты сохраняются в надлежащей тайне, к тому же пароли часто бывают групповыми. Во-вторых, такие улики и способ их нахождения не зафиксированы законодательно. Более того, эти улики не являются неотъемлемыми характеристиками личности, какими являются, например, подпись или отпечатки пальцев в криминалистике.

Поэтому для доказательств вины преступника или правонарушителя необходимо включить в законодательство нормы, дающие возможность использовать в целях доступа в АС средства аутентификации личности по характеристикам, присущим конкретному субъекту, какими являются за рубежом средства распознавания пользователей по голосу, отпечаткам пальцев, геометрии кисти руки, радужной оболочке глаз, динамическим характеристикам подписи и т.д.

При рассмотрении проблемы подтверждения личности правонарушителя с помощью технических средств возникают следующие вопросы:

- какими техническими средствами можно обеспечить подлинную аутентификацию пользователя АС при правомерном или несанкционированном доступе к информации?

- с какой вероятностью должен идентифицироваться пользователь АС в случае применения технических средств?

- какими методами или способами может быть признана подлинность пользователя АС?

И все же основная проблема правового регулирования вопросов безопасности информации лежит не в этой плоскости.

Любой закон будет действовать только при условии предусмотрения механизма его реализации в виде организационных структур, обеспечивающих выполнение положений этого закона на всех уровнях управления.

В этом смысле показательны законы Германии, Франции, директивы президента США по защите информации. Так, в Германии для реализации требований, правил и процедур по защите информации введен институт уполномоченных по защите, назначаемых законодательной властью, начиная от уровня федерального министерства внутренних дел и кончая уровнем администрации любой фирмы. Во Франции на республиканском уровне соответствующие функции по защите информации выполняются Национальной комиссией по информатике и свободам, а в США - руководящей группой по обеспечению безопасности.

Подобная иерархическая структура управления деятельностью по обеспечению безопасности информации предусмотрена в Законе [3] для координации, организационно-методического руководства деятельностью в этой области, контроля защищенности информации, осуществления других связанных с этим функций.

Правовые аспекты защиты информации наиболее тесно связаны с вопросами организации работ и процедурами технологического процесса обработки информации.

С помощью правовых норм должны быть решены такие вопросы, как отнесение информации к категориям открытого и ограниченного доступа, определение полномочий по доступу к информации, права должностных чип на установление и изменение полномочий, способы и процедуры доступа, порядок контроля, документирования и анализа действий персонала, ответственность за нарушение установленных требований и правил, а также соответствующие штрафные санкции. Предложения по структуре законодательного обеспечения в области защиты информации изложены в [7].

Административное регулирование и практическая деятельность в области защиты информации в нашей стране были связаны на начальном этапе своего развития, в основном, с защитой государственных секретов. Государственные секреты защищали, прежде всего, от утраты, утечки в традиционной сфере обращения документов, в меньшей степени придавая значение их защите при автоматизированной обработке. Вполне естественно поэтому, что не уделялось должного внимания защите от несанкционированного уничтожения или искажения информации в автоматизированных системах. Лишь в области передачи информации по линиям связи учитывалась возможность утечки секретной и навязывания ложной информации, и велись работы по их предупреждению. В результате к концу 80-х годов сложилась ситуация, когда на государственном уровне отсутствовали утвержденные нормативно-технические требования по защите информации от НСД.

Единственным официальным документом, в очень общем виде определявшим требования в этой области, была инструкция по секретному делопроизводству, в ряде разделов которой содержались некоторые рекомендации по вопросам организации автоматизированной обработки информации. Это не означало, однако, что в стране

не занимались серьезно вопросами защиты информации от НСД, но организована эта работа была и координировалась в лучшем случае на отраслевом уровне.

Для устранения этого недостатка по инициативе Гостехкомиссии СССР (ныне Гостехкомиссия России) была разработана Государственная научно-техническая программа по созданию средств вычислительной техники общего назначения в защищенном исполнении, в которой большое внимание уделялось проведению исследований и разработке нормативно-технических документов в области защиты информации от НСД.

Серьезным результатом интеграции в рамках одного государственного органа всего комплекса вопросов по защите информации стала разработка и становление государственной системы защиты информации, предусматривающей реализацию единой научно-технической политики по комплексной защите информации на всех уровнях управления [8].

Эта система предусматривает создание и функционирование органа управления государственной системой защиты информации в лице Гостехкомиссии, осуществляющей координацию деятельности органов и организаций в области защиты информации, обрабатываемой техническими средствами, организационно-методическое руководство этой деятельностью, разработку и финансирование научно-технических программ по защите информации, утверждения нормативно-технической документации, функции государственного органа по сертификации продукции по требованиям безопасности информации, лицензирование деятельности предприятий по оказанию услуг в этой области.

Деятельность по защите секретной информации в информационных системах должна осуществляться во взаимодействии с органами государственной безопасности. В этой работе Гостехкомисия должна опираться на ведущие научные центры страны, специализирующиеся в различных направлениях безопасности информации, и отраслевые и республиканские органы защиты информации, являющиеся следующим уровнем управления и связующим звеном с предприятиями и организациями, испытывающими потребность в защите информации.

На предприятиях в целях защиты информации в системах ее автоматизированной обработки должны создаваться службы обеспечения безопасности информации.

Государственная система защиты информации дополняется системой контроля защищенности информации в лине уполномоченных государством органов, осуществляющих обязательный контроль за выполнением требований по защите информации, являющейся собственностью государства. Такие контрольные органы могут предоставлять для собственников негосударственной конфиденциальной информации услуги по оценке соответствия уровня защищенности этой информации установленным требованиям.

Конкретная организационная структура государственной системы защиты информации может изменяться в зависимости от складывающейся в стране политической и экономической ситуации, роль Гостехкомиссии в этой системе может стать другой государственный орган управления.

Необходимость существования государственной системы защиты информации и соответствующих организационных структур подтверждается не только в условиях так

называемой административно-командной системы, но и в странах с развитыми рыночными отношениями. Зарождающаяся правовая основа защиты информации, приобретающая особенно большое значение в условиях сосуществования различных форм собственности, может опираться только на конкретные организационные структуры, осуществляющие законотворческую деятельность и являющиеся базой механизма реализации законов. Нельзя забывать, что и органы юстиции как неотъемлемая принадлежность любого государства, в случае противоправной деятельности по отношению к информации должны опираться на какие-то организационные структуры.

Важными элементами государственной системы защиты информации являются подсистема лицензирования деятельности предприятий по оказанию услуг в области защиты информации и подсистема сертификации средств вычислительной техники по требованиям безопасности информации. Функционирование указанных подсистем должно стимулировать разработку и внедрение современных, высококачественных технических средств и защитить потребителя продукции и услуг от недобросовестной работы исполнителя.

Подсистема лицензирования направлена на создание условий, при которых право заниматься работами по защите информации для стороннего заказчика представлено только организациям, имеющим на этот вид деятельности соответствующее разрешение (лицензию) [9].

Подсистема сертификации СВТ по требованиям безопасности ин-формации, являющаяся частью государственной системы защиты информации, одновременно составляет часть государственной системы сертификации продукции, действующей под управлением органов стандартизации [10].

Более детально вопросы сертификации и лицензирования в области защиты информации изложены в пособие [20].

Важным организационным документом государственной системы защиты информации является "Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники" [11]. Указанное положение устанавливает единый в стране порядок исследований, разработок, введения в действие и эксплуатации защищенных от НСД к информации СВТ и АС.

Положение определяет организационную структуру и порядок проведения работ, систему государственных нормативных актов, стандартов, руководящих документов по этой проблеме, порядок разработки и приемки защищенных СВТ и АС, порядок их эксплуатации и контроля защищенности. Система нормативно-технических документов, предусмотренная Положением, определяет работу в двух направлениях:

- разработка СВТ общего и специального назначения, защищенных от утечки, искажения или уничтожения информации, включая разработку программных и технических (в том числе криптографических) средств и систем защиты информации от НСД;

- разработка, внедрение и эксплуатация защищенных АС различного уровня и назначения, создаваемых как на базе защищенных СВТ, прошедших

сертификационные испытания, так и на базе несертифицированных средств и систем, например систем собственной разработки.

Исходя из практических потребностей, в Положении определены различные варианты разработки защищенных СВТ (в том числе программных и технических средств защиты информации от НСД), среди которых предусматривается разработка:

- защищенных общесистемных программных средств (ОС, СУБД, телемониторов, сетевых программных средств);

- защищенных программных средств на базе общесистемного программного обеспечения, находящегося в эксплуатации и поставляемого вместе с незащищенными СВТ предприятиями-изготовителями или Государственным фондом алгоритмов и программ;

- защищенных программных средств на базе импортных общесистемных программных прототипов, что особенно актуально в наши дни для ПЭВМ и ЛВС на их основе.

В Положении изложен также порядок разработки, внедрения и эксплуатации средств криптографической защиты информации (СКЗИ) от НСД.

Вопрос 2. РУКОВОДЯЩИЕ НОРМАТИВНО-ТЕХНИЧЕСКИЕ, МЕТОДИЧЕСКИЕ И ОРГАНИЗАЦИОННЫЕ ДОКУМЕНТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организационные документы, рассмотренные в предыдущем вопросе, представляют собой пакет нормативных подзаконных актов государственной системы зашиты информации, который дополняет и конкретизирует в организационном плане правовые акты.

Кроме них для нормальной деятельности в области безопасности информации необходим пакет нормативных документов технического характера: стандартов, руководящих документов, инструкций.

Как уже отмечалось, до последнего времени в области защиты информации от НСД в стране не существовало общегосударственных требований, хотя документ такого направления был разработан и введен в действие для стран-членов СЭВ.

Учитывая практическую потребность в такого рода документах в ряде отраслей промышленности стали появляться отраслевые руководящие методические и технические материалы по защите информации от НСД, в соответствии с которыми разрабатывались средства и системы разграничения доступа к информации.

Рассмотрим сначала ситуацию в данной области, сложившуюся в технически развитых странах. Так в США, например, в 1984 г. был принят в качестве государственного стандарта широко известный в мире документ "Критерии оценки доверенных вычислительных систем" [13] (так называемая "Оранжевая книга") и сопутствующее ему руководство по использованию в системах МО США (1985 г.), а несколько позже руководство по его применению для оценки защищенности сетей ЭВМ (1987 г.) и СУБД

(1989 г.). Именно в соответствии с "Оранжевой книгой" в США осуществляется сертификация СВТ по требованиям защиты информации от НСД. В Европейском сообществе в 1991 г. приняты собственные "Критерии оценки безопасности информационных технологий"[14], построенные на аналогичных принципах, в качестве основы которых использован документ, инициативно разработанный и согласованный четырьмя европейскими странами: Великобританией, Францией, Германией и Голландией.

Отечественным аналогом "Оранжевой книга" является Руководящий документ по стандартизации "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ" [15]. Этот документ устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований и может использоваться как методический материал для заказчиков и разработчиков СВТ при формировании и реализации требований по защите.

Показатели защищенности применяются к общесистемным программным средствам и операционным системам. Конкретные перечни (наборы) показателей определяют классы защищенности. Каждый показатель описывается совокупностью требований. Требования к показателям реализуются с помощью программно-технических средств, совокупность которых составляет комплекс средств защиты (КСЗ).

Концепция защиты СВТ и АС от НСД к информации предусматривает существование двух относительно самостоятельных и, следовательно, имеющих отличие направлений в проблеме защиты информации от НСД: направления, связанного с СВТ, и направления, связанного с АС.

Их отличие порождено тем, что СВТ разрабатываются и поставляются на рынок как элементы, из которых в дальнейшем проектируется АС. Следовательно, защищенность СВТ представляет собой потенциальную защищенность, т.е. свойство предотвращать или существенно затруднять НСД к информации, обрабатываемой в АС, построенной с использованием защищенных СВТ.

Но если защита СВТ обеспечивается только комплексом программно-технических средств, то защита АС обеспечивается как комплексом программно-технических средств, так и поддерживающих их организационных мер. Указанные отличия обусловили создание самостоятельных технических требований по защите информации, обрабатываемой в АС, от НСД в виде самостоятельного Руководящего документа по стандартизации - "Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации"[12], который может, также, использоваться в качестве нормативно-методического материала для заказчиков и разработчиков АС при формировании и реализации требований по защите.

Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации.

Дифференциация подхода к выбору методов и средств защиты определяется

важностью и уязвимостью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

К числу определяющих признаков, по которым производится группировка АС по классам, относятся: наличие в АС информации различного уровня конфиденциальности, уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации и режим обработки данных в АС (коллективный или индивидуальный).

В документе приведены условия использования в АС, предназначенной для обработки информации, являющейся собственностью государства и отнесенной к категории секретной, средств вычислительной техники, защищенность которых определяется по [15].

В качестве связующего терминологического звена для всех перечисленных выше документов можно привести Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа. Термины и определения" [16].

Перечисленной документацией не исчерпывается потребность данного направления работ. Это лишь та необходимая основа организационной, нормативно-технической и методической документации, без которой невозможно нормальное существование и развитие информатики, и обеспечение безопасности информационных ресурсов и самих средств вычислительной техники.

Вопрос 3. ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ И ПРОЦЕДУРЫ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

В предыдущем вопросе рассматривались, в основном, вопросы правового регулирования на уровне государственной власти и органов государственного управления. В этом вопросе рассмотрим проблему организации работ на уровне предприятия произвольной формы собственности, использующего в своей деятельности средства вычислительной техники для обработки информации, подлежащей защите. Именно на этом уровне возникает потребность в решении проблем безопасности информации, составляющей как государственную, так и коммерческую тайну, секреты производства (ноу-хау), а также безопасности самих автоматизированных систем, используемых, например, в управлении экологически опасными объектами.

Рассмотрим в целом организационные мероприятия и процедуры, используемые для решения проблем безопасности информации на всех этапах проектирования и эксплуатации автоматизированной системы.

Существенное значение при проектировании автоматизированных систем различного уровня и назначения придается предпроектному обследованию объекта автоматизации. На этой стадии параллельно с технико-экономическим обоснованием проектирования АС специальной группой обследования, назначенной приказом заказчика АС:

- устанавливается наличие или отсутствие секретной (конфиденциальной) информации в АС, подлежащей разработке, оценивается уровень конфиденциальности и объемы;

- определяются режимы обработки этой информации, тип АС, состав комплекса основных технических средств вычислительной техники (СВТ), общесистемные программные средства, предполагаемые к использованию в разрабатываемой АС;

- оценивается возможность использования имеющихся на рынке сертифицированных средств защиты информации;

- определяется степень участия персонала ВЦ, функциональных и производственных служб, научных и вспомогательных работников объекта автоматизации в обработке информации, характер взаимодействия между собой и со службой безопасности;

- определяются мероприятия по обеспечению режима секретности на стадии разработки.

Вполне естественно, что результаты предпроектного обследования в части наличия подлежащей защите информации и оценки ее уровня конфиденциальности и ценности могут базироваться только на документально оформленных перечнях сведений, будь то перечень сведений, подлежащих засекречиванию, или перечень коммерческих секретов, секретов производства.

Наличие таких перечней является необходимым условием, но недостаточным для решения вопроса об уровне конфиденциальности информации в АС. Для решения этого вопроса необходимо проанализировать структуру информационного обеспечения системы, необходимость наличия в ней защищаемых сведений и степень их интеграции, объемы и формы представления информации для пользователей и другие составляющие.

Основным результатом этой части анализа должна быть рекомендация о разработке (в случае необходимости) системы защиты секретной (конфиденциальной) информации (СЗСИ).

Важным с экономической точки зрения должно быть решение об использовании в составе СЗСИ имеющихся на рынке сертифицированных средств защиты информации или разработке специализированных средств собственными силами или с привлечением лицензированного предприятия.

Предпроектное обследование как законченная научно-техническая работа может быть поручена и специализированному предприятию, имеющему лицензию на этот вид деятельности, но и в этом случае анализ информационного обеспечения в части конфиденциальной информации целесообразно выполнять представителям заказчика при методической помощи специализированного предприятия.

На основании результатов предпроектного обследования разрабатывается аналитическое обоснование создания СЗСИ и раздел ТЗ на ее разработку.

В комплексе работ по созданию АС должна предусматриваться опережающая разработка и внедрение системы СЗСИ, реализуемой в виде подсистемы ЛС и включающей в себя комплекс организационных, программно-технических (в т.ч.

криптографических) средств, систем и мероприятий по защите информации от НСД. СЗСИ состоит из системной и функциональной частей. Системная часть является общей и применяется при разработке, внедрении и эксплуатации всех или большинства задач АС, функциональная часть обеспечивает защиту информации при решении конкретной задачи и специфична для нее. При разработке защищенной АС следует руководствоваться требованиями по защите информации от НСД в АС различных классов.

Прежде чем перейти к рассмотрению организационных мероприятий и процедур по обеспечению безопасности на других стадиях проектирования, ввода в действие и эксплуатации АС, рассмотрим организационную структуру обеспечения безопасности информации и основные функции служб и лиц, задействованных в этой работе.

Учитывая различные возможности предприятия-заказчика АС, можно рассмотреть несколько вариантов организационной структуры обеспечения безопасности информации на разных стадиях создания АС. Например, на стадии проектирования АС они могут базироваться на двух полярных вариантах организации разработки: выполняемой в целом своими силами или силами лицензированного предприятия. Вполне естественно, что конкретный вариант находится где-то между ними, и, следовательно, организационная структура может отличаться от типовой.

Предусматривается, что на предприятии в случае самостоятельной разработки АС, научно-техническое руководство и непосредственную организацию работ по созданию СЗСИ интегрированной АС осуществляет главный конструктор этой системы, а по типам АС - главный конструктор этих систем, научные руководители тем, начальники объектов ЭВТ или другие должностные лица, обеспечивающие научно-техническое руководство всей разработкой соответствующей АС.

Разработка СЗСИ АС осуществляется подразделением, разрабатывающим на предприятии АС, группой или отдельными специалистами по разработке мер и средств защиты (в дальнейшем подразделение разработки средств и мер защиты) или специализированными предприятиями, имевшими лицензию на этот вид деятельности.

На подразделения разработки средств и мер защиты информации возлагается разработка и внедрение системной части СЗСИ (адаптация, настройка сертифицированных программно-технических средств, разработка в необходимом случае специализированных средств, соответствующих мероприятий и документации), а также разработка требований к функциональной части СЗСИ, которая создается специалистами-разработчиками функциональных подсистем АС.

Важное место в системе организации работ по обеспечению безопасности информации на предприятиях занимают так называемые специальные научно-технические подразделения (СИТИ) - службы защиты информации, основной направленностью которых являются организация работ по выявлению возможностей и предупреждению утечки информации, методическое руководство и участие в разработке требований по защите информации от НСД, аналитического обоснования необходимости создания СЗСИ, согласование выбора СВТ (в том числе общесистемного программного обеспечения), программно-технических средств и систем защиты.

В случае привлечения для разработки СЗСИ специализированных предприятий, функции и задачи различных служб могут изменяться и перераспределяться, но координация должна остался за предприятием-заказчиком АС.

Кроме того, в обеспечении безопасности информации, особенно на стадии эксплуатации АС, задействованы службы обеспечения безопасности информации или секретный орган, службы администратора АС, о которых будет сказано далее. Все указанные службы активно взаимодействуют в целях достижения эффективной разработки и эксплуатации АС и ее СЗСИ.

Для эффективной и надежной с точки зрения обеспечения безопасности информации работ АС необходимо правильно организовать разрешительную систему доступа пользователей к информации в АС, т.е. предоста-вить пользователям право работать с той информацией, которая необходима им для выполнения своих функциональных обязанностей, установить их полномочия по доступу к информации.

Это означает, что необходимо определить и оформить порядок установления уровня полномочий пользователей, а также круга лиц, которым это право предоставлено, установить правила разграничения доступа, регламентирующие права доступа субъектов к объектам, т.е. не только, кто из пользователей АС и их программ допускается к тем или иным программам, файлам, записям, но и какие действия при этом они могут осуществлять (читать, писать, выполнять). Все это оформляется службой безопасности информации или администратором АС в виде матрицы доступа или иных правил разграничения доступа.

Среди организационных мероприятий по обеспечению безопасности информации важное место занимает охрана объекта, на котором расположена защищаемая АС (территория, здания, помещения, хранилища информационных носителей), путем установления соответствующих постов технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение СВТ, информационных носителей, а также НСД к СВТ и линиям связи.

Следует отметить, что в последнее время в направлении физической защиты помещений, самих СВТ, информационных носителей наблюдается смещение акцентов в сторону использования в этих целях средств защиты, основанных на новых принципах. Например, доступ в помещения разрешается и контролируется с помощью системы, оконечными устройствами которой проверяются различного рода индивидуальные жетоны, магнитные и электронные карточки (используемые в виде ключа для входа в помещение или для аутентификации в системе). Защита от утечки секретной или иной конфиденциальной информации, записанной на магнитных носителях, осуществляется путем использования средств криптозащиты.

Технология обработки информации в АС различна и зависит от используемых СВТ, программных средств, режимов работы. Не вдаваясь в особенности технологического процесса, обусловленные различиями в технике, программном обеспечении и другими причинами, можно констатировать, что основной характерной особенностью, связанной с обработкой секретной или иной подлежащей защите информации, является функционирование системы защиты информации от НСД (СЗИ НСД) как комплекса программно-технических средств и организационных решений. Данный комплекс предусматривает:

- учет, хранение и выдачу пользователям информационных носителей, паролей, ключей;

- ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа);

- оперативный контроль за функционированием СЗСИ;

- контроль соответствия общесистемной программной среды эталону и приемку включаемых в АС новых программных средств;

- контроль за ходом технологического процесса обработки информации путем регистрации анализа действий пользователей, сигнализации опасных событий.

Перечисленные составляющие являются функциональной направленностью службы безопасности информации, администратора АС. Они фиксируются, с одной стороны, в положениях об этих службах и общей организационной документации по обеспечению безопасности информации ("Положение о порядке организации проведения на предприятии работ по защите информации в АС", "Инструкция по защите информации, обрабатываемой в АС предприятия (подразделения предприятия)"), а с другой стороны, в проектной документации СЗИ НСД (инструкциях администратору АС, службе безопасности информации, пользователю АС).

В заключение следует отметить, что некоторые другие аспекты правовой защиты информации изложены в пособиях [17, 20].

ЛЕКЦИЯ 6
НАЗНАЧЕНИЕ, СТРУКТУРА, МЕТОДЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебные вопросы:

1. Правовая основа информационной безопасности.
2. Система правового регулирования информационной безопасности.

Вопрос 1. ПРАВОВАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Государственная система правового регулирования информационной безопасности представляет собой совокупность федеральных и иных органов управления, осуществляющих воздействие на информационные правоотношения с помощью юридических форм, методов и средств и направленное на обеспечение ИБ информационных ресурсов.

Создание правовой основы ИБ в целях обеспечения эффективного использования информационных ресурсов и защиты интересов государства является безотлагательной задачей и непосредственно связано с защитой конституционных прав и свобод личности, обеспечением безопасности России и надежным функционированием всех систем управления. Информационная безопасность включает:

- защиту общества от отрицательных последствий информатизации;

- обеспечение ответственности нарушителей;

- соблюдение прав человека, интересов личности, организаций, государства, правопорядок отношений в области информатизации;

- использование техники и технологий в этой сфере.

Для обеспечения ИБ необходимо наличие соответствующих органов, организаций, ведомств и обеспечение их эффективного функционирования. Совокупность этих органов составляет систему безопасности.

В соответствии с Законом о безопасности систему безопасности, а, следовательно, и ИБ образуют:

- органы законодательной, исполнительной и судебной властей;

- государственные, общественные и иные организации и объединения;

- граждане, принимающие участие в обеспечении безопасности;

- законодательство, регламентирующее отношения в сфере безопасности.

Указанный Закон закрепляет лишь организационную структуру системы безопасности. Сама же система обеспечения безопасности намного шире и затрагивает не только правовые аспекты. Поэтому при ее формировании необходимо учитывать не только субъекты безопасности, но и:

- объекты ИБ Российской Федерации;

- связи и отношения между ними, организацию их деятельности;

- формы, методы и средства обеспечения ИБ.

Анализ действующих нормативных правовых актов позволил выделить в качестве субъектов обеспечения безопасности, представляющих организационную структуру системы ИБ, следующие компоненты:

- федеральные органы государственной власти;

- органы государственной власти субъектов РФ;

- органы местного самоуправления, решающие задачи в области обеспечения ИБ в пределах своей компетенции;

- государственные и межведомственные комиссии и советы, специализирующиеся на решении проблем обеспечения ИБ;

- структурные и межотраслевые подразделения по защите конфиденциальной информации органов государственной власти Российской Федерации, а также структурные подразделения предприятий, осуществляющие работы с использованием сведений, отнесенных к государственной тайне, или специализирующиеся на проведении работ в области защиты информации;

- научно-исследовательские, проектные и конструкторские организации, выполняющие работы по обеспечению ИБ;

- учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения ИБ;

- граждане, общественные и иные организации, обладающие правами и обязанностями по обеспечению ИБ в установленном законом порядке.

Основными функциями рассмотренной системы ИБ Российской Федерации являются:

- разработка и реализация стратегии обеспечения ИБ;

- создание условий для реализации прав граждан и организаций на разрешенную законом деятельность в информационной сфере;

- оценка состояния ИБ в стране; выявление источников внутренних и внешних угроз ИБ; определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз;

- координация и контроль деятельности системы обеспечения ИБ;

- организация разработки федеральных и ведомственных программ обеспечения ИБ

и координация работ по их реализации;

- проведение единой технической политики в области обеспечения ИБ;

- организация фундаментальных, поисковых и прикладных научных исследований в области ИБ;

- обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации и сертификации средств защиты информации;

- осуществление международного сотрудничества в сфере ИБ, представление интересов Российской Федерации в соответствующих междуна-родных организациях.

Основной целью системы ИБ является защита конституционных прав и свобод граждан.

Анализ структуры и функций системы ИБ, с учетом сложившейся системы разделения властей, позволил выявить субъекты обеспечения ИБ и их полномочия.

Государство является главным и основным субъектом обеспечения ИБ в лице Президента РФ, Федерального собрания РФ, Правительства РФ, органов судебной власти, Совета безопасности РФ, Федеральной службы по техническому и экспортному контролю (ФСТЭК России, специализированных федеральных органов исполнительной власти России (ФСБ, ФСО, ФПС, СВР).

Общее руководство субъектами обеспечения ИБ в рамках определенных полномочий осуществляет Президент РФ. К его полномочиям в сфере обеспечения ИБ относятся:

- осуществление руководства и взаимодействия органов государственной власти;

- контроль и координация деятельности органов обеспечения ИБ;

- определение жизненно важных интересов Российской Федерации в информационной сфере;

- определение внутренних и внешних угроз этим интересам;

- определение основных направлений стратегии обеспечения ИБ.

Федеральное Собрание РФ формирует на основе Конституции РФ законодательную базу в сфере ИБ.

Правительство РФ в пределах своих полномочий:

- обеспечивает руководство государственными органами;

- организует и контролирует разработку и реализацию мероприятий по обеспечению ИБ министерствами и другими подведомственными ему органами.

Органы судебной власти также являются субъектами обеспечения ИБ – они обеспечивают судебную защиту граждан, права которых были нарушены в связи с деятельностью по обеспечению ИБ, осуществляют правосудие по делам о преступлениях в информационной сфере.

Особая роль в обеспечении безопасности государства, в том числе информационной,

принадлежит Совету безопасности РФ – это конституционный орган, не обладающий статусом федерального органа исполнительной власти, но наделенный достаточными полномочиями в сфере обеспечения безопасности. Совет безопасности является единственным совещательным органом при Президенте РФ, создание которого предусмотрено действующей Конституцией РФ. Основными задачами Совета безопасности РФ являются:

- разработка проектов указов и иных правовых актов по основным направлениям внутренней, внешней и военной политики в сфере обеспечения безопасности;

- разработка предложений по координации деятельности федеральных органов государственной власти в процессе реализации принятых решений в сфере обеспечения ИБ;

- разработка предложений по совершенствованию системы обеспечения ИБ;

- осуществление государственной политики в сфере ИБ.

Не менее важное место принадлежит Федеральной службе по техническому и экспортному контролю (ФСТЭК России) – являясь федеральным органом исполнительной власти, осуществляет:

- единую государственную политику в области технической защиты информации;

- утверждает нормативно-методические документы по технической защите информации;

- межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную или служебную тайну;

- прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

- предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней;

- специальные работы по технической защите информации и др.

К системе специализированных федеральных органов исполнительной власти, обеспечивающих безопасность, относится и Федеральная служба безопасности РФ (ФСБ России), которая осуществляет государственное управление в сфере обеспечения безопасности РФ и реализует основные направления деятельности органов ФСБ. К ее основным задачам относятся:

- информирование государственных органов власти об угрозах безопасности Российской Федерации;

- обеспечение защиты сведений, составляющих государственную тайну;

- проведение во взаимодействии с другими службами мероприятий по обеспечению безопасности и др.

Федеральная служба охраны РФ (ФСО России) также относится к субъектам обеспечения безопасности. Ее основной функцией является обеспечение безопасности

лиц, которые подлежат государственной охране. Кроме этого ФСО, как субъект обеспечения безопасности, в том числе некоторых аспектов информационной, необходимо, в части обеспечения правительственной связи и информации, является составной частью сил обеспечения безопасности РФ и входит в систему органов федеральной исполнительной власти, которые обеспечивают высшие органы государственной власти Российской Федерации, органы государственной власти субъектов РФ, центральные органы федеральной исполнительной власти, Совет безопасности РФ, организации, предприятия, учреждения специальными видами связи и информации, а также совместно с ФСБ участвуют в организации и обеспечении и деятельности центральных органов федеральной исполнительной власти, организаций, предприятий, учреждений средствами криптографической и инженерно-технической безопасности и шифрованной связи в России и ее учреждениях за ру-бежом, а также осуществляют в рамках своих полномочий государственный контроль за этой деятельностью.

К субъектам обеспечения безопасности относятся и другие силовые федеральные министерства и ведомства. Так в составе ФСБ, Федеральная пограничная служба РФ (ФПС России) в рамках осуществления своих основных функций по охране государственной границы, территориального моря, континентального шельфа, государственных границ государств – участников СНГ также решает задачи обеспечения ИБ.

Обеспечение безопасности Российской Федерации на территории зарубежных государств и соответственно ИБ осуществляется Службой внешней разведки РФ (СВР России). В ее компетенцию входит осуществление разведывательной деятельности в политической, экономической, экологической и иных сферах.

Одной из специфических является охранительная функция государства. Выполнение значительной ее части принадлежит органам внутренних дел, которые являются также субъектами обеспечения безопасности. Министерство внутренних дел РФ (МВД России) возглавляет систему органов внутренних дел России, в которую входят территориальные органы МВД России в субъектах Федерации – министерства внутренних дел республик в составе России, Главное управление, управления и отделы внутренних дел, внутренние войска. В нее также входят различные службы, подразделения, учебные заведения, предприятия, учреждения, организации. Министерство осуществляет государственное управление в сфере защиты прав и свобод человека и гражданина, реализует основные направления деятельности органов внутренних дел. Его основные задачи:

- разработка и принятие в пределах своей компетенции мер по защите прав и свобод человека и гражданина, защите объектов независимо от форм собственности, обеспечение общественного порядка и общественной безопасности;

- принятие мер по совершенствованию деятельности органов внутренних дел;

- совершенствование нормативно-правовой базы деятельности органов внутренних дел;

- совершенствование работы с кадрами, их профессиональной подготовки и др.

Таким образом, в организационную основу системы ИБ РФ входят Президент РФ, Федеральное Собрание РФ, Правительство РФ, Совет безопасности РФ, федеральные

органы исполнительной власти, органы судебной власти, органы государственной власти субъектов РФ, органы местного самоуправления. Кроме того, государство в соответствии с действующим законодательством обеспечивает безопасность каждого гражданина, как на территории РФ, так и ее пределами.

Другие органы государственного управления (министерства, ведомства) в пределах своей компетенции:

- определяют перечень охраняемых сведений;

- обеспечивают разработку и осуществление технически и экономически обоснованных мер по защите информации на подведомственных предприятиях;

- организуют и координируют проведение НИОКР в области защиты информации в соответствии с государственными (отраслевыми) программами;

- разрабатывают отраслевые документы по защите информации;

- контролируют выполнение на предприятиях отрасли установленных норм и требований по защите информации;

- создают отраслевые центры по защите информации и контролю эффективности принимаемых мер;

- организуют подготовку и повышение квалификации специалистов по защите информации.

Вопрос 2. СИСТЕМА ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для осуществления указанных в первом вопросе функций в составе органов государственного управления функционируют научно-технические подразделения (центры) защиты информации и контроля.

На предприятиях, выполняющих оборонные и иные секретные работы, функционируют научно-технические подразделения защиты информации и контроля, координирующие деятельность в этом направлении научных и структурных производственных подразделений предприятия, участвующие в разработке и реализации мер по защите информации, осуществляющие контроль эффективности этих мер. Кроме того, в отраслях промышленности и регионах страны создаются и функционируют:

- лицензионные центры, осуществляющие организацию и контроль за лицензионной деятельностью в области оказания услуг по защите информации;

- органы по сертификации СВТ и средств связи;

- испытательные центры по сертификации конкретных видов продукции по требованиям безопасности информации;

- органы по аттестации объектов информационной безопасности.

При создании государственной системы организационно-правового регулирования выявились новые проблемы ИБ и защиты информации. Это защита:

- права личности на частную жизнь (в том числе защита персональных данных), конституционных прав личности на тайну переписки, переговоров, личную тайну;

- коммерческой тайны в предпринимательской и финансовой деятельности путем законодательного установления механизмов защиты и обеспечения "добросовестной конкуренции";

- технических и программных средств информатики от злоумышленника, ошибочных действий персонала и техногенных воздействий.

Реализация механизмов защиты перечисленных объектов безопасности стала актуальной проблемой именно в настоящее время. Объективными условиями для развития этих аспектов проблемы безопасности являются:

- переход к рыночной модели экономики, требующий создания эффективной защиты предпринимателя от криминогенных угроз и недобросовестной конкуренции, в том числе промышленного шпионажа;

- необходимость защиты национального информационного ресурса при включении наших систем в международные системы и сети;

- рост степени возможного ущерба при отказе оборудования АСУ потенциально опасных производств в результате некомпетентных действий персонала или техногенных катастроф;

- возникновение новых форм общественных отношений в сфере бизнеса (электронные деньги, электронная подпись, электронная биржа, электронное соглашение с правом юридической силы и т. д.).

Новыми эти вопросы являются потому, что, расширив число участников правоотношений, мы начинаем учитывать интересы не только государства, но и коллективов и частных лиц. В результате появляется необходимость правового регулирования их отношений. Интересы юридических лиц, действующих в различных условиях рыночных отношений, в значительной степени отличаются от прежней монопольной позиции государства. Прежде всего, тем, что в основе этих интересов лежит острая необходимость обезопасить себя (свой коммерческий интерес) от риска и угроз. Важным является то, что в этом случае государство, как было сказано раннее, само начинает выступать в качестве субъекта, также требующего защиты от риска и угроз. Если же эти угрозы реализуются, то субъекту причиняется ущерб в виде прямых финансовых потерь или упущенной выгоды.

По фактам преступлений в финансовой сфере были собраны статистические данные последних лет. Анализ наиболее крупных преступлений, связанных с хищением валютных и денежных средств во Внешэкономбанке по поддельным финансовым документам, дает основания полагать, что статистика финансовых компьютерных преступлений не будет отличаться от аналогичной статистики в западных странах. Близкими оказываются и побудительные мотивы этих преступлений.

Таким образом, к настоящему времени сформировались направления, требующие законодательной поддержки:

- защита персональных данных;

- борьба с компьютерной преступностью, в первую очередь в финансовой сфере;

- защита коммерческой тайны и обеспечение благоприятных условий для предпринимательской деятельности;

- защита государственных секретов;

- создание системы взаимных финансовых расчетов в электронной форме с элементами цифровой подписи;

- обеспечение безопасности АСУ потенциально опасных производств;

- страхование информации и информационных систем;

- сертификация и лицензирование в области безопасности, контроль безопасности информационных систем;

- организация взаимодействия в сфере защиты данных со странами – членами СНГ и другими государствами.

Анализ современного состояния информационной безопасности в России показывает, что ее уровень в настоящее время не в полной мере соответствует жизненно важным потребностям личности, общества и государства.

К негативным факторам, осложняющим решение задач обеспечения ИБ, относятся:

- обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных ограничений на ее распространение;

- несовершенство нормативно-правовой базы, отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве;

- слабое обеспечение органов государственной власти и управления полной, достоверной и своевременной информацией, неразвитость информационных отношений в сфере предпринимательства;

- недостаточная защищенность государственного информационного ресурса и слабость мер по обеспечению сохранности государственных секретов в органах государственной власти и управления;

- необеспеченность прав граждан на информацию, манипулирование информацией, вызывающее неадекватную реакцию населения и ведущее в ряде случаев к политической нестабильности в обществе.

Такое положение дел в области обеспечения ИБ требует безотлагательного решения ряда ключевых проблем. Их решение должно сводиться к следующему:

- формированию нормативной правовой базы обеспечения ИБ, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, нормативному закреплению ответственности должностных лиц и граждан по соблюдению требований ИБ;

- формированию системы ИБ и как ее части системы правового регулирования, обеспечивающей реализацию государственной политики в этой области;

- разработке механизмов реализации прав граждан на информацию;

- исследованию форм и способов цивилизованного воздействия государства на формирование общественного сознания.

Таким образом, очевидно, что для формирования эффективной системы правового регулирования ИБ и защиты информации необходима концепция, которая позволит проводить в стране единую, обеспечивающую сбалансированность интересов личности и государства политику в области ИБ.

Несовершенство законодательства по вопросам информации и информатизации в России определяет необходимость комплексного подхода к формированию и разработке единой концепции правового обеспечения этого процесса с учетом соотношения законодательства в области информатизации и всей системой законодательства РФ.

При создании правовой основы процесса информатизации необходимо учитывать:

- состояние и состав международных норм в области информатизации;

- состояние отечественного законодательства в этой и смежных областях;

- формирование системы законодательства с охватом всех ее уровней, обеспечением преемственности и совместимости норм в законах разного уровня – конституционных, общих, специальных;

- последовательный выход на развитие ведомственных и местных нормативных актов с опорой на законодательную основу;

- создание механизмов, обеспечивающих организацию, применение, действенность законодательной базы информатизации.

Направления создания правовой базы должны затрагивать все уровни законодательства России. Например, конституционно должны быть закреплены и оформлены права граждан, организаций, государства на информацию и последовательно обеспечены во всех законах – о собственности, правах граждан, гражданстве, предпринимательстве и т. д.

Вопросы информации, информационного обеспечения обязательно должны присутствовать в законах о разделении компетенции и правовом статусе различных государственных систем, органов и организаций государственного устройства по вертикали и горизонтали.

Нормативные правовые акты в области информатизации должны быть ориентированы на создание условий в организации и упорядочении самой информации, управление государственными информационными ресурсами, обеспечение процесса включения современных технологий во все направления информатизации, создание систем защиты информации и систем ее обработки, установление гарантий и т.д. Кроме федерального законодательства вопросы информатизации должны быть учтены в законодательстве субъектов РФ.

Важное место в правовом обеспечении информатизации должны занимать подзаконные нормативные акты, отражающие процессы информатизации и защиты информации.

Обязательной составной частью рассматриваемой структуры системы законодательства является правоохранительное законодательство, включающее нормы об ответственности за правонарушение при работе с информацией.

Рассмотрим более подробно проблему формирования законодательства в области информации. Существует проблема, связанная с характеристикой самого информационного законодательства и как его части – законодательства в сфере ИБ.

Из анализа некоторых работ следует, что весь массив актов, который относится к информационному законодательству, характеризуется по-разному: «отрасль права», «информационное право», «компьютерное право». Распространена трактовка «специальное право». Следуя логике авторов данного определения, «специальной» следует признать любую отрасль законодательства. Некоторые ученые считают, что использование понятия «информационное право» преждевременно . Они исходят из следующих позиций. В теории права четко сформулированы критерии, позволяющие рассматривать тот или иной нормативно-правовой массив в качестве отрасли права. Отрасль права объединяет ряд правовых институтов; для нее характерно наличие ряда базовых законов, выделение принципов, разделение на общую и особенную части, наличие методов правового регулирования, механизма применения. Одним из важных показателей выделения законодательного массива в самостоятельную отрасль права является наличие самостоятельных принципов и так называемой критической массы нормативных правовых актов. Исходя из этого, правильным решением этой проблемы является отнесение нормативно-правового массива по информатизации к понятию «отрасль законодательства».

Отрасль законодательства – это массив нормативных правовых актов в определенной сфере, не достигший уровня отрасли права, хотя и обладающий определенной степенью единства и достаточно большим количеством нормативных правовых актов, входящих в него. Отрасль законодательства включает в себя не только законы как акты высшей юридической силы, но и подзаконные нормативные правовые акты.

Ряд авторов выдвигают концепцию «компьютерного» права. Они относят к этой области правовое регулирование общественных отношений, связанных с производством и использованием компьютеров в различных областях. Концепция «компьютерного» права вызывает ряд возражений. Прежде всего, объекты «компьютерного» права не образуют целостного единства. К тому же концепция «компьютерного» права не находит поддержки у законодателя.

Наряду с этим существует еще одна проблема – формирование научных представлений об объекте информационного законодательства. Этим объектом являются информационные отношения. Тенденцию обособления информационных отношений отмечает Ю.М. Батурин. В.А. Копылов выделяет конституционные информационные отношения, т. е. отношения, объективно существующие на уровне Конституции РФ. А.Б. Агапов предпринял попытку классификации информационных отношений. Понятие и термин «информационные отношения» получил законодательное закрепление. Под ними понимаются отношения по поводу сбора, накопления, хранения и использования информации. Представляется, что это

определение является неполным, так как не охватывает все информационные процессы, по поводу которых и возникают информационные правоотношения.

Информационные правоотношения – это отношения, возникающие по поводу сбора, обработки, накопления, хранения, поиска, распространения, использования информации, информационных ресурсов и регулируемые нормами информационного законодательства. Указанные отношения возникают при осуществлении информационных процессов. Таким образом, отнесение массива нормативных правовых актов в сфере информации и информатизации к понятию «отрасль законодательства» является, по-нашему мнению, вполне обоснованным. На основе проведенного анализа можно утверждать, что использование понятия «информационное право» вполне оправдано и для наименования соответствующей дисциплины.

Законодательство в сфере ИБ должно состоять из базового закона и набора нормативных правовых актов, формируемых в его развитие. Ведь регулировать всю совокупность отношений в области ИБ одним законом нецелесообразно; в этом случае оно окажется громоздким, перегруженным частными нормами. Кроме того, при формировании структуры законодательства в информационной сфере необходимо учитывать, как минимум, две особенности.

Первая особенность заключается в принципах построения законодательства в сфере информации и информатизации. Межпарламентская ассамблея государств – участников СНГ приняла Рекомендательный законодательный акт «О принципах регулирования информационных отношений в государствах – участниках Межпарламентской Ассамблеи». В этом акте впервые были определены следующие принципы:

- законодательное закрепление права граждан, организаций, государства на свободный поиск, получение, использование и распространение информации и гарантии реализации этого права, за исключением случаев, установленных национальным законодательством;

- установление правового режима информации;

- обеспечение доступности информации, не отнесенной законом в установленном порядке к информации с ограниченным доступом;

- установление правовых форм защиты информации и гарантий ИБ, а также защиты авторских и иных прав в области информационных отношений.

Принимая во внимание эти принципы, необходимо отметить, что они применимы и для законодательства в сфере ИБ. Однако для информационного законодательства первые два принципа являются частными. Они могут применяться только для информационных правоотношений.

Для информационного законодательства должны быть сформулированы следующие принципы:

- равенства субъектов информационных отношений;

- ИБ и защиты информации;

- свободы информации с установлением ограничений доступа к отдельным видам информации и информационных ресурсов.

Вторая особенность заключается в учете существующих классификаций и систематизаций нормативных правовых актов. Система нормативных правовых актов современных государств неоднородна. Это объясняется особенностями форм государственного правления, многовековыми традициями отдельных стран, национальными и другими факторами. Тем не менее, подавляющее большинство нормативно-правовых актов строится по признаку степени юридической силы акта. Акты нижестоящих органов государственной власти в интересах стабильности общественной жизни, ее оптимальной организованности должны соответствовать предписаниям актов вышестоящих органов. Все коллизии, противоречия между подзаконными актами в цивилизованном государстве решает закон, обладающий высшей юридической силой.

Таким образом, при формировании законодательства в сфере ИБ необходимо учитывать не только его принципы, но и принципы всего информационного законодательства.

ЛЕКЦИЯ 7
ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ КАК ФИНАНСОВО-ПРАВОВАЯ КАТЕГОРИЯ

Учебные вопросы:

1. Правовая основа экономической безопасности
2. Основные угрозы экономической безопасности

Вопрос 1. ПРАВОВАЯ ОСНОВА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Проблема определения экономической безопасности с позиций права является также достаточно сложной. Ведь так сложилось, что до недавнего времени эта категория преимущественно рассматривалась в рамках экономической науки. Не случайно ее представителями отмечается, что экономическая безопасность как категория экономической теории, хотя и имеет свой предмет и специфические методы исследования, тесно связана с такими традиционными экономическими понятиями, как "экономический рост" и "устойчивость социально-экономической системы". Более того, экономическая безопасность определяется ими как компонент антикризисного управления экономикой <1>.

Впрочем, единство взглядов на экономическую безопасность отсутствует и среди экономистов. В частности, понимается она как некое состояние экономики, проявляющее способность к самовыживанию в условиях возникновения внутренних и внешних угроз, а также функционирования в непредсказуемой окружающей среде и трудно прогнозируемых факторов <2>. Предлагается рассматривать экономическую безопасность и как совокупность условий и факторов, обеспечивающих независимость национальной экономики, ее стабильность и устойчивость, способность к постоянному обновлению и самосовершенствованию <3>.

Отдельными авторами экономическая безопасность трактуется как "важнейшая качественная характеристика экономической системы, определяющая ее способность поддерживать нормальные условия жизнедеятельности населения, устойчивое обеспечение ресурсами развития народного хозяйства, а также последовательную реализацию национально-государственных интересов России" <4>.

Существует и такая точка зрения, в соответствии с которой экономическая безопасность той или иной системы - это совокупность свойств состояния ее производственной подсистемы, обеспечивающая возможность достижения целей всей системы <5>. В данном случае экономическая безопасность видится специалистам как некая обеспечительная способность применительно к экономике.

Несколько отличный подход усматривается в других научных работах. Например, экономическая безопасность определяется в них как способность экономики

обеспечивать эффективное удовлетворение общественных потребностей на национальном и международном уровнях. Иными словами, экономическая безопасность понимается как совокупность внутренних и внешних условий, благоприятствующих эффективному динамичному росту национальной экономики, ее способности удовлетворять потребности общества, государства, индивида, обеспечивать конкурентоспособность на внешних рынках, гарантировать от различного рода угроз и потерь <6>.

В этой связи не без оснований отмечается, что в общем смысле экономическая безопасность чаще всего понимается как важнейшая качественная характеристика экономической системы, способность ее поддерживать нормальные условия жизнедеятельности общества, государства, населения страны, устойчивое обеспечение необходимыми ресурсами хозяйства. Однако такой подход вряд ли может быть признан исчерпывающим, поскольку категория "экономическая безопасность" должна охватывать помимо характеристики экономической системы целый ряд параметров общественной и государственной деятельности, прежде всего применительно к избранной методологии и методике исследования, уровень эффективности государственного управления, его различных ветвей власти и их институтов и структур, в том числе судебной власти. С содержательной же и организационной стороны экономическая безопасность предполагает деятельность по защите экономики страны от нежелательных и опасных по возможным последствиям воздействий <7>.

Наряду с этим экономическую безопасность предлагается рассматривать и через состояние защищенности экономики. При этом в данном случае это не только защищенность соответствующих национальных интересов, но и готовность, а также способность институтов власти создавать механизмы реализации и защиты национальных интересов развития отечественной экономики, поддержание социально-политической стабильности общества <8>.

Наиболее развернутое определение подобного рода дано Г.В. Коржовым, который определяет экономическую безопасность как такое состояние хозяйства и институтов власти, при котором обеспечивается подлинная защита национальных общенародных интересов от актуальных и потенциальных угроз в целях преодоления кризиса, сохранения главных цивилизационных ценностей, природных богатств и основных производственных ресурсов, создания условий для устойчивого и социально направленного развития, поддержания политической стабильности и оборонной достаточности страны в случае реализации даже критических сценариев развития внутренней и международной ситуации <9>.

Как мы видим, эти определения сформулированы прежде всего исходя из экономической сущности рассматриваемого феномена. В этой связи констатируется, что подходы к определению содержания понятия "экономическая безопасность", встречающиеся в экономической литературе, имеют в своей основе понимание ее как некоторого состояния экономики, при котором обеспечиваются экономическое благополучие нации, устойчивый экономический рост, стабильность внутреннего рынка, защита экономических интересов на национальном и международном уровнях <10>.

Тем не менее указанные выше обстоятельства, впрочем, совсем не исключают возможности рассмотрения экономической безопасности и с позиций права,

поскольку она получила нормативно-правовое закрепление, а правовые средства занимают важное место в системе ее обеспечения.

Конечно, совсем абстрагироваться от экономической материи, принимая во внимание специфику рассматриваемого института, вряд ли возможно, поэтому при определении экономической безопасности, очевидно, придется сочетать категории, относимые на счет различных научных сфер. Тем не менее при выработке соответствующего правового понятия определенным подспорьем послужат теоретические выкладки, которые получены нами в предыдущей части исследования. В данном случае имеются в виду экономические составляющие, имеющие место в структуре национальных интересов, вызовов и угроз, а также средств противодействия, которые в общем виде уже представлены нами выше. Кроме того, за основу соответствующего юридического понятия нами принимается тезис о том, что экономическая безопасность является основной составляющей (подсистемой) национальной безопасности Российской Федерации. По крайней мере, при формулировании искомого определения следует исходить из того, что экономическая безопасность - это не только защищенность национальных интересов, но и готовность и способность институтов власти создавать механизмы реализации и защиты национальных интересов развития отечественной экономики <11>.

Правоведами также предложено несколько научных версий определения экономической безопасности. В частности, экономическая безопасность понимается отдельными авторами как защита экономики страны от опасных воздействий внешнего и внутреннего характера. Эти воздействия могут быть вызваны как стихийными рыночными процессами, так и сознательным поведением субъектов, удовлетворяющих личные или корпоративные интересы. При этом опасными являются такие воздействия, которые приводят к ухудшению экономического положения страны до критического уровня, за которым следует разрушение существующей экономической системы или социальное потрясение, дестабилизирующее все сферы общественной жизнедеятельности <12>.

Из всего вышеизложенного следует, что правоведы склонны определять экономическую безопасность через состояние защищенности экономики от неких внутренних и внешних угроз и вызовов, причиняющих вред экономическим интересам общества, государства и личности и приводящих к негативным для них последствиям. Тем не менее, полагаем, что понятие экономической безопасности следует рассматривать несколько шире, включая в него правовую составляющую.

В этой связи следует согласиться с выводом о том, что экономическая безопасность с юридической точки зрения включает в себя две составляющие: во-первых, это такое состояние подлежащих правовому регулированию общественных отношений, при котором поведение субъектов права в сфере производства, обмена, распределения и потребления материальных и духовных благ соответствует установленным правовым предписаниям; и во-вторых, это такое состояние законодательства, регулирующего сферу экономических отношений, при котором оно соответствует требованиям экономической безопасности <13>.

С учетом всего изложенного экономическую безопасность можно определить как составную часть национальной безопасности Российской Федерации, представляющую собой такое состояние и развитие урегулированных правом общественных отношений в сфере экономики, которое обеспечивает непрерывное и

эффективное производство, обмен, распределение и потребление материальных и нематериальных благ в интересах личности, общества и государства.

Необходимо учесть, что выработка основных положений экономической безопасности изначально пришлась на период, когда Российская Федерация переживала сложный исторический период становления новых социально-экономических отношений. Переход к новым формам государственного управления происходил в условиях постоянного дефицита и противоречивости правовой базы, регулирующей экономические отношения, отставания законодательства от реально происходящих в обществе процессов. В международных отношениях страна сталкивалась со стремлением промышленно развитых стран, крупных иностранных корпораций использовать ситуацию в Российской Федерации и государствах - участниках Содружества Независимых Государств в своих экономических и политических интересах. Все это подвигло к осуществлению целенаправленной деятельности по обеспечению экономической безопасности страны и ее граждан на основе единой государственной стратегии.

В целях обеспечения национальных интересов Российской Федерации в области экономики и поддержания экономической безопасности страны Указом Президента Российской Федерации от 29 апреля 1996 г. N 608 одобрена Государственная стратегия экономической безопасности Российской Федерации (Основные положения) (далее - Государственная стратегия экономической безопасности) <14>. Этот правовой акт исходит из того, что экономическая безопасность является составной частью национальной безопасности Российской Федерации, поэтому в нем развиваются и конкретизируются соответствующие положения Концепции национальной безопасности с учетом национальных интересов в области экономики.

В качестве основной цели экономической безопасности продекларировано обеспечение такого развития экономики, при котором создались бы приемлемые условия для жизни и развития личности, социально-экономической и военно-политической стабильности общества и сохранения целостности государства, успешного противостояния влиянию внутренних и внешних угроз. Без обеспечения экономической безопасности практически невозможно решить ни одну из задач, стоящих перед страной, как во внутригосударственном, так и в международном плане.

Государственная стратегия экономической безопасности исходит из того, что ее реализация должна создать необходимые условия для достижения общих целей национальной безопасности и обеспечить:

- защиту гражданских прав населения, повышение уровня и качества его жизни, гарантирующих социальный мир в стране и спокойствие в обществе;

- эффективное решение внутренних политических, экономических и социальных задач, исходя из национальных интересов;

- активное влияние на процессы в мире, затрагивающие национальные интересы России.

Внешнеэкономическая направленность экономической безопасности заключается в эффективной реализации преимуществ международного разделения труда, устойчивости развития страны в условиях ее равноправной интеграции в мирохозяйственные связи, недопущении критической зависимости Российской

Федерации от зарубежных стран или их сообществ в жизненно важных вопросах экономического сотрудничества. В данном случае находит подтверждение вывод о том, что необходимость защиты национальных интересов стала диктовать необходимость ограждения своего национального хозяйства от негативного воздействия целого ряда факторов, вызванных происходящими в мировой экономике процессами <15>. Ведь сохранение экономической безопасности государств с точки зрения влияния неблагоприятных процессов в мировом хозяйстве становится важнейшей задачей как на уровне отдельных государств, так и мирового сообщества в целом <16>.

В Государственной стратегии экономической безопасности также определены ее объекты, что является важным с точки зрения понимания ее правовой сущности. В частности, в качестве таковых определены личность, общество, государство и основные элементы экономической системы, включая систему институциональных отношений при государственном регулировании экономической деятельности.

Попытки определить объекты экономической безопасности предпринимались и на теоретическом уровне. Так, отдельные специалисты относят к ним народное хозяйство в целом, отдельные регионы страны, сферы и отрасли хозяйства, юридических и физических лиц как субъектов хозяйственной деятельности <17>.

Полагаем, что экономическая безопасность действительно существует как на общегосударственном уровне, уровне регионов и муниципальных образований, так и на уровне отдельных хозяйствующих субъектов. В данном случае следует заметить, что термин "экономическая безопасность" рядом авторов используется применительно к частным субъектам - коммерческим и некоммерческим организациям - с позиций обеспечения их экономической безопасности <18>. Полагаем, что такой подход вполне допустим. Тем не менее в рамках данного исследования мы ограничимся рассмотрением экономической безопасности государства в целом, поскольку она имеет определяющее значение для всех уровней.

Основываясь на содержании Государственной стратегии экономической безопасности, можно сделать вывод, что в целом оценка состояния экономической безопасности осуществляется на основе: характеристики внешних и внутренних угроз как совокупности условий и факторов, создающих опасность для жизненно важных экономических интересов личности, общества и государства; определения и мониторинга факторов, подрывающих устойчивость социально-экономической системы государства. В свою очередь, указанные факторы устанавливаются посредством определения критериев и параметров, характеризующих национальные интересы в области экономики и отвечающих требованиям экономической безопасности Российской Федерации.

Обеспечение же экономической безопасности предполагает формирование экономической политики, институциональных преобразований и необходимых механизмов, устраняющих или смягчающих воздействие факторов, подрывающих устойчивость национальной экономики. Все это должно осуществляться посредством принятия комплекса конкретных мер, реализуемых на основе качественных индикаторов и количественных показателей, включая макроэкономические, демографические, внешнеэкономические и др.

В качестве важнейших показателей положения дел в экономике, эффективности

проводимой экономической политики выступают так называемые индикаторы экономической безопасности. В данном случае следует исходить из того, что экономика, как наиболее сложная система, имеет тысячи показателей, характеризующих ее состояние, которые используются на макро- и мезоуровне для анализа и прогнозирования угроз экономической безопасности. Однако представителями экономической науки признано целесообразным использование в качестве основных 19 индикаторов, которые отражают наиболее важные сферы экономической безопасности в реальном и финансовом секторах экономики, в социальной сфере. К ним, в частности, относятся:

- объем валового внутреннего продукта (ВВП);

- доля в ВВП инвестиций в основной капитал;

- доля в ВВП расходов на оборону;

- доля затрат на гражданскую науку в ВВП;

- доля инновационной продукции в общем объеме промышленной продукции;

- доля машиностроения и металлообработки в промышленном производстве;

- доля во всем населении лиц с денежными доходами ниже прожиточного минимума;

- отношение доходов 10% наиболее обеспеченного к доходам 10% наименее обеспеченного населения;

- уровень безработицы;

- уровень монетизации;

- внешний долг;

- внутренний долг;

- доля расходов на обслуживание госдолга в общем объеме расходов федерального бюджета;

- дефицит федерального бюджета;

- уровень инфляции;

- объем золотовалютных резервов;

- отношение выплат по внешнему долгу к объему годового экспорта;

- валовой сбор зерна;

- доля продовольствия, поступившего по импорту, в общем объеме продовольственных ресурсов.

Отклонение от пороговых значений указанных индикаторов, которые представляют собой предельные, абсолютные либо относительные их значения, как раз и указывает на опасность перерастания отдельных угроз в системный кризис, дестабилизацию экономики и политической жизни общества <19>.

Вопрос 2. ОСНОВНЫЕ УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Как уже отмечалось, в системе обеспечения экономической безопасности первостепенное значение имеет выявление возможных угроз, поскольку без этого выработка и реализация мер, ее обеспечивающих, невозможна. Задача выявления подобных угроз изначально являлась сложной. Специалистами отмечается, что весь спектр угроз и рисков в сфере экономики настолько широк, что в определенном смысле охватывает все сферы хозяйства и направления развития российской экономики. Вместе с тем основными источниками угроз экономической безопасности Российской Федерации на современном этапе являются накопленные диспропорции в структуре экономики, а также резкое повышение роли внешнего фактора и неопределенность происходящих в мире процессов <20>.

В самой Государственной стратегии экономической безопасности к числу "наиболее вероятных угроз экономической безопасности" отнесены:

- увеличение имущественной дифференциации населения и повышение уровня бедности;

- деформация структуры экономики;

- возрастание неравномерности социально-экономического развития регионов;

- криминализация общества и хозяйственной деятельности.

Проведем анализ указанных угроз с целью определения полноты их учета и сохранения их актуальности (степени опасности) в современной действительности. Это необходимо в первую очередь потому, что рассматриваемая Государственная стратегия экономической безопасности формулировалась и утверждалась в период, приходящийся на такое состояние экономики в Российской Федерации, которое по ряду позиций уже существенно отличается от современного ее состояния.

В частности, в Государственной стратегии экономической безопасно-сти к числу угроз, посягающих на социальный мир и общественное согласие, отнесены увеличение имущественной дифференциации населения и повышение уровня бедности. При этом к числу ее негативных факторов относятся:

- расслоение общества на узкий круг богатых и преобладающую массу бедных, не уверенных в своем будущем людей;

- увеличение доли бедных слоев населения в городе по сравнению с деревней;

- рост безработицы;

- задержка выплаты заработной платы;

- остановка и закрытие предприятий.

Проблема бедности не является новой для Российской Федерации, поскольку, как отмечают специалисты, социально-экономические и правовые условия разных исторических периодов создавали различные причины и механизмы ее формирования. Вместе с тем и в постсоветский период, как это ни прискорбно,

сохраняются в определенной степени тяжелейшее социально-экономическое положение бедных и невосприимчивость права к реалиям социальной дифференциации <21>. Крайние на этот счет суждения сводятся, например, к тому, что если в конце 60-х гг. доля малообеспеченных ("бедных") составляла 29,6%, в конце 70-х гг. - 32,1%, в конце 80-х - 30,7%, то в результате "шоковой терапии" проблема бедности как самостоятельная исчезнет, замещаясь проблемой экономической разрухи, падения уровня экономического развития и вследствие этого - жизненного уровня населения в целом. Бедной становится как бы страна в целом <22>.

Справедливости ради следует заметить, что общая численность населения с денежными доходами ниже величины прожиточного минимума, по данным Федеральной службы государственной статистики, сократилась в Российской Федерации с 42,3 млн. человек в 2000 г. до 25,2 млн человек в 2008 г. <23>. Следует принять во внимание и тот факт, что последнее время в Российской Федерации отмечается неуклонный рост реальных доходов населения (в 2010 г. в среднем реальные доходы выросли на 12,5%). Тем не менее все еще сохраняющийся большой разрыв в доходах состоятельных и малоимущих граждан реально угрожает экономике.

Дополнительную угрозу составляет просроченная задолженность по заработной плате, которая, по данным Федеральной службы по труду и занятости, на 1 февраля 2011 г. составила более 4,8 млрд. руб., увеличившись по сравнению с 1 января т.г. на 644 млн. руб. (15,5%). В целом задолженность по заработной плате в общем объеме просроченной задолженности составила в среднем 31% <24>.

К числу угроз экономической безопасности относится также деформация структуры российской экономики, которая обусловлена такими факторами, как:

- усиление топливно-сырьевой направленности экономики;

- отставание разведки запасов полезных ископаемых от их добычи;

- низкая конкурентоспособность продукции большинства отечествен-ных предприятий;

- свертывание производства в жизненно важных отраслях обрабатывающей промышленности, прежде всего в машиностроении;

- снижение результативности, разрушение технологического единства научных исследований и разработок, распад сложившихся научных коллективов и на этой основе подрыв научно-технического потенциала;

- завоевание иностранными фирмами внутреннего рынка Российской Федерации по многим видам товаров народного потребления;

- приобретение иностранными фирмами российских предприятий в целях вытеснения отечественной продукции как с внешнего, так и с внутреннего рынка;

- рост внешнего долга Российской Федерации и связанное с этим увеличение расходов бюджета на его погашение.

Большинство из указанных угроз сохранило свою актуальность, хотя индекс промышленного производства (в январе 2011 г. он составил 108,4% по сравнению с аналогичным периодом прошлого года) <25> и увеличение ВВП до 26 621,3 млрд.

руб. (106,7%) в целом свидетельствуют о позитивных изменениях в российской экономике, произошедших за последнее время.

Тем не менее представляется, что степень опасности некоторых из указанных угроз уже существенно снизилась. Например, состояние внешнего долга Российской Федерации, по данным Банка России, за последние годы характеризуется его существенным снижением, следствием чего является уменьшение расходов бюджета на его обслуживание. По состоянию на 2000 г. государственный долг Российской Федерации действительно был огромен и составлял 158,6 млрд. долл. США, однако в течение последующих пяти лет Российская Федерация успешно осуществила ускоренное его погашение. Только в течение 2009 г. задолженность органов государственного управления снизилась на 27% - с 97,4 млрд. до 71,4 млрд. долл. США. В том же году Российская Федерация досрочно выплатила остающуюся часть долга МВФ, составлявшую на тот момент 3,3 млрд. долл. США. С января по октябрь 2010 г. задолженность перед странами - членами Парижского клуба кредиторов также досрочно сокращена с 22,2 млрд. до 0,6 млрд. долл. США <26>.

Возрастание неравномерности социально-экономического развития регионов складывается из таких негативных факторов, как:

- объективно существующие различия в уровне социально-экономического развития регионов, наличие депрессивных, кризисных и отсталых в экономическом отношении районов на фоне структурных сдвигов в промышленном производстве, сопровождающихся резким уменьшением доли обрабатывающих отраслей;

- нарушение производственно-технологических связей между предприятиями отдельных регионов Российской Федерации;

- увеличение разрыва в уровне производства национального дохода на душу населения между отдельными субъектами Российской Федерации.

На региональный аспект экономической безопасности обращают внимание и специалисты. По их мнению, экономическая подсистема региональной безопасности включает в себя комплекс мер, препятствующих возникновению и реализации угроз для региональной экономики в целом, экономического положения жителей и организаций различных субъектов Российской Федерации <27>. Например, из-за значительной (до 40%) доли импорта продуктов питания обращается внимание на возможную утрату продовольственной безопасности в отдельных регионах <28>. Тем не менее нельзя не учитывать позитивные изменения, которые за последние годы также произошли в региональной экономике. Так, по данным статистики, в 2010 г. по сравнению с предшествующим годом рост основных экономических показателей отмечен в большинстве субъектов Российской Федерации (от 69 до 98%). Наиболее высокий индекс промышленного производства (более 120%) зафиксирован в Калининградской, Сахалинской, Ленинградской областях, Агинском Бурятском автономном округе. Вместе с тем в 11 субъектах Российской Федерации отмечено снижение производства.

Инвестиции в региональный капитал в 2010 г. в целом по Российской Федерации выросли на 13,7%, при этом наибольший прирост (более чем на 50%) отмечен в таких регионах, как Республика Хакасия, Архангельская и Томская области, Агинский Бурятский и Корякский автономные округа <29>. Тем не менее существенные

диспропорции на уровне региональных экономик все еще сохраняются.

В ряду угроз экономической безопасности числится также криминализация общества и хозяйственной деятельности, что в первую очередь обусловлено факторами, к числу которых относятся:

- рост безработицы, поскольку значительная часть преступлений совершается лицами, не имеющими постоянного источника дохода;

- сращивание части чиновников государственных органов с организованной преступностью, возможность доступа криминальных структур к управлению определенной частью производства и их проникновения в различные властные структуры;

- ослабление системы государственного контроля, что привело к расширению деятельности криминальных структур на внутреннем финансовом рынке, в сфере приватизации, экспортно-импортных операций и торговли.

Криминализация экономики как негативный фактор отмечается многими специалистами <30>. В свое время А.Н. Ларьковым обращалось внимание на то, что в период проведения экономических реформ страну захлестнули крупномасштабные мошеннические операции в кредитно-финансовой системе: массовый обман населения создателями разного рода финансовых "пирамид" и фондов, нецелевое использование кредитов, присвоение средств, полученных по договорам, неплатежи <31>. Криминологами экономическая преступность определена как совокупность преступных посягательств, причиняющих вред охраняемым законом экономическим интересам общества и граждан вследствие совершения хищений, хозяйственных и корыстных должностных преступлений <32>. Особенность заключается в том, что вред, причиненный экономическим преступлением, составляет сущность преступного последствия, что отличает его от вреда, причиненного правонарушением, ответственность за которое предусмотрена иными нормами права (гражданским, административным и др.). В результате совершения преступного деяния посредством воздействия на объект преступления происходят изменения, которые могут быть только социально вредными <33>.

Особого внимания заслуживает существование такого опасного явления, как теневая (неформальная) экономика, которая формируется в рамках экономических отношений, складывающихся на основе противоправного поведения <34>. По сути, теневая экономика представляет собой хозяйственную деятельность, которая осуществляется вне государственного учета и контроля и не получает отражения в официальной статистике. Последствия теневой экономической деятельности неоднозначны, однако ее негативное воздействие заключается в том, что она позволяет осуществлять антисоциальное распределение доходов в обществе в пользу относительно малочисленных привилегированных групп, сопровождающееся уменьшением благосостояния общества в целом. Кроме того, подобная деятельность фактически разрушает систему централизованного управления экономикой <35>.

Данные официальной статистики прямо указывают на наличие исключительно опасных угроз экономической безопасности, которые находят проявление в форме преступных посягательств. В 2010 г. (по сравнению с предыдущим годом) на 11,8% возросло число преступлений экономической направленности, выявленных

правоохранительными органами. Всего выявлено 489,6 тыс. преступлений данной категории, удельный вес этих преступлений в общем числе зарегистрированных составил 12,7%. При этом треть (35,6%) в общем числе выявленных преступлений экономической направленности составили тяжкие и особо тяжкие преступления. Совокупный материальный ущерб от указанных преступлений (по оконченным уголовным делам) составил 127,6 млрд руб. <36>.

На теоретическом уровне в качестве основных рисков для Российской Федерации в экономической сфере обозначаются:

- нерациональный выбор приоритетов и пропорций развития экономики, усиление структурной деформации экономики страны;

- криминализация экономики и утечка капитала из страны;

- снижение производственного потенциала и низкая инвестиционная активность;

- возможность энергетического кризиса;

- превышение пределов открытости национальной экономики в условиях международной глобализации;

- неблагоприятная экономическая конъюнктура, снижение мировых цен на энергоносители;

- внешний долг, создающий опасность обострения финансового кризиса;

- низкая конкурентоспособность продукции;

- снижение объемов сельскохозяйственного производства, потеря продовольственной независимости <37>. Очевидно, что многие перечисленные риски соответствуют уже рассмотренным нами выше позициям.

В свою очередь, основными причинами, вызывающими возникновение указанных угроз, в соответствии с Государственной стратегией экономической безопасности, являются неустойчивость финансового положения предприятий, неблагоприятный инвестиционный климат, сохранение инфляционных процессов и другие проблемы, связанные с финансовой дестабилизацией в экономике. Эти негативные факторы в рамках данного исследования требуют особого внимания, поскольку их нейтрализация, по нашему мнению, в первую очередь и предполагает использование финансово-правовых средств.

Финансовая устойчивость большого числа предприятий в Российской Федерации, к сожалению, остается все еще невысокой. Хотя в 2010 г. сальдированный финансовый результат (прибыль минус убыток) организаций (без субъектов малого предпринимательства, банков, страховых и бюджетных организаций) в действующих ценах составил +3845,9 млрд. руб., при этом 64,1 тыс. организаций получили прибыль в размере 4161,5 млрд. руб., однако 27,1 тыс. организаций имели убыток на сумму 315,6 млрд. руб.

Что касается инвестиционного климата, то с недавнего времени отток капитала из Российской Федерации существенно сократился и уже довольно отчетливо обозначается изменение к лучшему. Во всяком случае, по данным Федеральной

службы государственной статистики, поступление иностранных инвестиций в Российскую Федерацию в 2010 г. увеличилось на 2,7% - до 55,1 млрд. долл. США, при этом прямые иностранные инвестиции составили 13,7 млрд. долл. США, что на 4,6% больше, чем в 2009 г. Инвестиции в основной капитал в целом по Российской Федерации по состоянию на январь 2011 г. составили 238,2 млрд. руб., что на 23,2% больше по сравнению с январем 2010 г.

Все еще довольно высокий уровень инфляции действительно отрицательно сказывается на положении дел в экономике. Индекс потребительских цен составил в 2010 г. 8,2% <38>.

Как мы видим, положение дел в современной экономике Российской Федерации требует внесения определенных коррективов в обозначенные в Государственной стратегии экономической безопасности положения. При этом помимо пересмотра степени опасности отдельных угроз следует вести речь и о новых угрозах и вызовах экономической безопасности, которые в свое время не нашли в ней отражения. Полагаем, что к ним, во всяком случае, следует отнести негативные факторы, имеющие место в финансовой сфере, включая нецелевое использование бюджетных средств, масштабное уклонение от уплаты налогов, фиктивные финансовые операции и легализацию преступно нажитых доходов.

О наличии негативных факторов в бюджетной сфере красноречиво свидетельствуют результаты деятельности Счетной палаты Российской Федерации в 2009 г. В указанный период только этим независимым органом государственного финансового контроля по итогам 520 проведенных кон-трольных мероприятий Правительству Российской Федерации, Минфину России, главным распорядителям средств федерального бюджета, иным участникам бюджетного процесса направлено 440 представлений. В органы прокуратуры, иные правоохранительные органы направлено 93 материала проверок, по которым возбуждено 257 уголовных дел. Выявлено нарушений законодательства в финансово-бюджетной сфере на сумму 122,7 млрд. руб. Устранено финансовых нарушений на сумму 2,2 млрд. руб. В том же периоде объем нецелевого использования бюджетных средств составил 1,1 млрд. руб., блокировано и возмещено средств на сумму 0,3 млрд. руб. <39>.

К числу явных угроз экономической безопасности относятся уклонение от уплаты налогов, незаконное возмещение налога на добавленную стоимость (НДС) и сохраняющаяся из года в год недоимка. Так, задолженность по налогам и сборам в бюджетную систему Российской Федерации, учитываемая с момента ее возникновения (без учета задолженности по уплате пеней и налоговых санкций), по состоянию на 1 января 2011 г. составила 757,4 млрд. руб. По сравнению с 1 января 2010 г. удалось достичь сокращения недоимки на 0,4%, в том числе по налогу на прибыль организаций - на 5,9%, акцизам - на 2,8%. Однако при этом увеличилась недоимка на добычу полезных ископаемых - в 5,8 раза, по налогу на добавленную стоимость - на 3,3%, акцизам на дизельное топливо - в 3,3 раза, на автомобильный бензин - в 2 раза, табачную продукцию - на 24%, алкогольную продукцию с объемной долей этилового спирта свыше 25%. Задолженность по уплате пеней и налоговых санкций (штрафов) на 1 января составила 745,8 млрд. руб. <40>.

Фиктивные финансовые операции и "отмывание денег" также представляют собой опасную угрозу экономической безопасности Российской Федерации. Так, по данным Федеральной службы по финансовому мониторингу, лишь за I полугодие 2010 г.

федеральная база данных увеличилась почти в 2 раза по сравнению с 2008 г., получено более 3 млн. сообщений об операциях с денежными средствами или иным имуществом, в том числе около 1,6 млн. сообщений - об операциях, выделенных самими финансовыми организациями как подозрительные. В правоохранительные органы направлено более 3 тысяч материалов на сумму около 1 трлн. руб. <41>.

Безусловно, указанные выше негативные факторы следует рассматривать в ряду других угроз экономической безопасности. В данном случае их губительное воздействие в первую очередь направлено на финансовые интересы общества и государства.

Библиографический список:

<1> Богомолов В.А. Экономическая безопасность. М., 2006. С. 4 - 5.

<2> Сенчагов В. О сущности и основах стратегии экономической безопасности России // Вопросы экономики. 1995. N 1. С. 98.

<3> Абалкин Л. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. 1998. N 12. С. 5.

<4> Бухвальд Е., Гловацкая Н., Лазуренко С. Макроаспекты экономической безопасности: факторы, критерии, показатели // Вопросы экономики. 1994. N 12. С. 25.

<5> Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура, проблемы // Вести Московского университета. Сер. 6. Экономика. 1995. N 3.

<6> Архипов А., Городецкий А., Михайлов Б. Экономическая безопасность: оценки проблемы, способы обеспечения // Вопросы экономи-ки. 1994. N 12.

<7> Тропин С.А. Экономическая безопасность России // Законодательство и экономика. 2004. N 5.

<8> Экономика: Учебник / Под ред. И.А. Архипова, А.Н. Несте-ренко, Л.К. Большаковой. М., 1999. С. 11.

<9> Коржов Г.В. Экономическая безопасность России: внешние связи. М., 1996. С. 9.

<10> Степенко В.Е., Чернова О.А. Экономическая безопасность в системе национальной безопасности России: сущность, спектр угроз и обуславливающих их возникновение факторов // Юридический мир. 2006. N 5.

<11> Экономическая и национальная безопасность: Учебник / Под ред. Е.А. Олейникова. М., 2004. С. 132.

<12> Кирюшин А.В., Плотников С.В. Правовые аспекты обеспе-чения экономической безопасности Российской Федерации // История госу-дарства и права. 2006. N 9.

<13> Гладких Р.Б. Обеспечение безопасности предпринимательской деятельности в системе мер, обеспечивающих экономическую безопасность государства //

Юридический мир. 2006. N 10.

<14> Собрание законодательства РФ. 1996. N 18. Ст. 2117.

<15> Огнев А.П. Международная экономическая безопасность: проблемы и пути решения. М., 1989. С. 5 - 14.

<16> Кистерский Л.Л., Гайдучок И.Г., Полунеев Ю.В. Международная экономическая безопасность: внешнеторговый, валютно-финансовый и энергетический аспекты / Отв. ред. Г.Н. Клименко. Киев, 1991. С. 5 - 6.

<17> Савин В.А. Некоторые аспекты экономической безопасности России // Международный бизнес России. 1995. N9.

<18> Бабкин В. Оценка потенциального заемщика с позиции экономической безопасности // Банковское дело в Москве. 2005. N 1, N 2; Кишеня В. Деловая разведка как необходимый инструмент обеспечения экономической безопасности бизнеса // Управление персона-лом. 2006. N 7; Комиссарова Я.В. Об использовании полиграфа в целях обеспечения экономической безопасности предприятия // Банковское право. 2006. N 2; Морозюк Ю.В. Критерии оценки экономической безопасности некоммерческих организаций // Бухгалтерский учет в бюджетных и некоммерческих организациях. 2006. N 10; Чалдаева Л.А. Организационно-экономические аспекты безопасности функционирования хозяйствующих субъектов // Бухгалтерский учет в бюджетных и некоммерческих организациях. 2004. N 20.

<19> Экономическая безопасность России: Общий курс. Учебник / Под ред. В.К. Сенчагова. 2-е изд. М., 2005. С. 75 - 90.

<20> Потапов В.Я. Оценка и прогноз опасностей и угроз современной России // Право и безопасность. 2003. N N 3 - 4.

<21> Федорова О.Г. Бедность в России (проблемы ее историко-правового анализа в постсоветском пространстве) // История государства и права. 2006. N 8.

<22> Римашевская Н.М. Бедность и маргинализация населения // СОЦИС. 2004. N 4. С. 34.

<23> См.: http://www.gks.ru.

<24> См.: http://www.rostrud.info.

<25> См.: http://www.gks.ru.

<26> См.: http://www.cbr.ru.

<27> Кирьянов А.Ю. Экономическая безопасность как особое направление обеспечения региональной безопасности в современном Российском государстве // Адвокатская практика. 2006. N 1.

<28> Колесников В.М. Каждому региону нужен "пас-порт безопасности" // Право и безопасность. 2004. N 4.

<29> См.: http://www.gks.ru.

<30> Амбросьев С.В. Некоторые аспекты противодействия криминальной экономике

// Российский следователь. 2006. N 6; Дмитриев О.В. Понятие экономической преступности в современной криминологии // Адвокатская практика. 2005. N 4; Кошаева Т.О. Вред, причиняемый экономическими преступлениями // Журнал российского права. 2002. N 8; Никитина И.А. Экономическая преступность в банковской сфере // Банковское право. 2006. N 2; Рахматуллин М.А., Вадюхина Р.Р. Социально-экономические причины и факторы развития теневой экономики в России // Безопасность бизнеса. 2005. N 4.

<31> Ларьков А.Н. Экономическая преступность и уголовный закон // Преступность и закон. Тезисы конференции. М., 1996. С. 43.

<32> Петров Э.И., Марченко Р.Н., Баринова Л.В. Криминологическая характеристика и предупреждение экономических преступлений. М., 1995. С. 12.

<33> Кошаева Т.О. Вред, причиняемый экономическими преступлениями // Журнал российского права. 2002. N 8.

<34> Попов Ю.Н., Тарасов М.Е. Теневая экономика в системе рыночного хозяйства: Учебник. М., 2005. С. 7 - 8.

<35> Латов Ю.В., Ковалев С.Н. Теневая экономика: Учеб. пособ. / Под ред. В.Я. Кикотя, Г.М. Казиахмедова. М., 2006. С. 14 - 18.

<36> Состояние преступности в России за 2010 год. М.: ГИАЦ МВД России, 2007. С. 71.

<37> Акимов В.А. Оценка и прогноз стратегических рисков России: теория и практика // Право и безопасность. 2004. N 1.

<38> См.: http://www.gks.ru.

<39> См.: http://www.ach.gov.ru.

<40> См.: http://www.akm.ru.

<41> См.: http://www.kfm.ru.

ЛЕКЦИЯ 8
АКМЕОЛОГИЧЕСКИЙ ПОТЕНЦИАЛ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Учебные вопросы:

1. Потенциал корпоративной безопасности.
2. Условия повышения потенциала корпоративной безопасности.

Введение

Функционирование системы корпоративной безопасности оказывается детерминировано ее потенциалом, который понимается с точки зрения акмеологического подхода как имманентно присущая организации возможность сохранять продуктивность деятельности и структуры при воздействии внешних и внутренних угроз. Рассматриваются структура потенциала, взаимосвязь с акмеологическими характеристиками персонала, векторы его развития.

Современная акмеология предоставляет широкие возможности для изучения феноменологии активного социального субъекта, закономерностей вершинных достижений. На стадии зрелости субъект приобретает свою качественную определенность, превращаясь из группы в общность, из простой совокупности людей в их целостное объединение, из суммы отдельных "я" в интегрированное "мы".

Показателем ставшей субъектности выступает превращение группы из потенциального "субъекта - в себе" в действительный "субъект - для себя", что выражается в самосознании, самодеятельности, внутренней сплоченности, деятельностном самоопределении и активности [1]. Организация является субъектом социальных отношений (удовлетворяет всем признакам субъектности), следовательно, в процессе социальной деятельности появляются интегративные системные феномены, и корпоративная безопасность оказывается одним из них [13].

Вопрос 1. ПОТЕНЦИАЛ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

Корпоративная безопасность (КБ) организации с точки зрения акмеологии может быть представлена в виде сложной модели, выявляющей изменение, развитие исходного состояния реального объекта ("оригинала" - по терминологии М. Вартофского), его переход от "стартового" к идеальному, "вершинному" состоянию. Модель выявляет изменение способа организации объекта от наличного к более оптимальному уровню. Желательное идеальное целевое состояние или качество проектируется (А.А. Деркач) согласно теоретическим, методологическим, гуманистическим принципам и -

одновременно - достигается практически заданными критериями, определяемыми системой функционирования личности - в качестве участника и субъекта всех сфер социальной и личной жизни, в том числе - профессиональной. В этом контексте потенциал (от лат. potentia - сила) удобно рассматривать как источники, возможности, средства, запасы, которые могут быть использованы для решения какой-либо задачи, достижения определенной цели; возможности отдельного лица, общества, государства в определенной области (напр., экономический потенциал).

Рассматривая потенциал корпоративной безопасности, отмечаем, что сама КБ оказывается интегративным организационным феноменом, производным определенной структуры, состоящей из ряда элементов. Проиллюстрируем сущность корпоративной безопасности через указание ее цели. Главной целью обеспечения корпоративной безопасности предприятия является достижение максимальной стабильности его функционирования, а также создание основы и перспектив роста для выполнения целей организации, вне зависимости от объективных и субъективных угрожающих факторов (негативных воздействий, факторов риска).

Выделяют следующие элементы корпоративной безопасности организации:

- финансовая безопасность рассматривает и регулирует вопросы финансово-экономической состоятельности предприятия, устойчивости к банкротству, определяет параметры платежеспособности и другие "денежные" характеристики;

- силовая безопасность занимается режимами, физической охраной объектов и личной охраной руководства, противодействием криминалу, взаимодействием с правоохранительными и другими государственными органами;

- информационная безопасность основана не только на защите собственной информации, в том числе конфиденциальной, но и проводит деловую разведку, информационно-аналитическую работу с внешними и внутренними субъектами и т.д.;

- технико-технологическая безопасность предполагает создание и использование такой технической базы, оборудования и основных средств производства и таких технологий и бизнес-процессов, которые усиливают конкурентоспособность предприятия;

- правовая безопасность подразумевает всестороннее юридическое обеспечение деятельности предприятия, грамотную правовую работу с контрагентами и властью, решение иных правовых вопросов;

- кадровая безопасность - процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом;

- суть экологической безопасности ясна без дополнительных комментариев.

Будучи имплицитно слитыми в едином поле корпоративной безопасности, эти элементы интегрируются в систему, и для корпоративной безопасности появляются два сущностных системных признака - стабильность и устойчивость организации. Они определяют то, насколько организация окажется устойчива к воздействию внутренних или внешних угроз, сохраняя при этом стабильность в структуре, функциях, кадрах и др. элементах. Это - сущность потенциала корпоративной безопасности.

Если потенциал сравнивать с возможностью, то ключевым свойством возможности, вероятно, можно считать ее актуальность для личности в момент совершения акта целенаправленного действия. Ведущим свойством потенциала можно считать вероятность реализации ресурсов в случае необходимости. Более того, если наличие возможности можно объективно наблюдать, то наличие потенциала можно только предполагать до момента его реализации. Следовательно, именно критические ситуации в организационной жизнедеятельности позволяют увидеть наличие потенциала корпоративной безопасности.

Если возможности организации проявляются в непосредственно наблюдаемой ситуации, то потенциал формируется, накапливается, развивается нередко в скрытой от наблюдения форме и только после этого обнаруживается в актуальной ситуации. Поэтому понятие "потенциал" находится в неразрывной связи с категорией "развитие", что обусловливает его скрытую динамическую природу. Потенциал существует именно как возможность, которая носит скрытый характер до момента ее обнаружения, когда потенциал "вызывается" на поверхность бытия силой обстоятельств (Н.А. Коваль, Р.П. Мильруд, К.В. Петров и др.).

Важными для понимания сущности потенциала являются взгляды В.Ж. Келле о том, что потенциал взаимосвязан с деятельностью. Он не существует сам по себе как некая обособленная от деятельности сущность, а материализуется в разных видах человеческой деятельности. Потенциал, таким образом, всегда имеет деятельностную природу (Б.Г. Ананьев, Т.И. Артемьева, Д.А. Леонтьев, В.Н. Марков, С.Л. Рубинштейн, Д.Н. Узнадзе и др.). Это связывает воедино деятельность с обнаружением, развитием и реализацией потенциала. Продолжая эту мысль, можно заметить, что потенциал непосредственно связан с механизмами овладения деятельностью, включая необходимые для этого навыки, умения и деятельностные компетенции.

Достаточно активно понятие "трудовой потенциал работника" используется в современном менеджменте и отчасти в социологии. При этом можно выделить следующие основные тенденции. В рамках первой из них потенциал рассматривается как совокупная характеристика определенной социальной общности (например, организации - А.А. Лобанов, А.А. Мерцалов, Ж.М. Галль, М. Хучек и др.). В рамках второй потенциал понимают более широко, и тогда речь идет о человеческих ресурсах, кадровом потенциале органов власти (Н.М. Байков) [2]. При этом в менеджменте также рассматривается индивидуальный трудовой потенциал работника (Ю.Г. Одегов и П.В. Журавлев) [18].

В.Н. Марков ввел понятие "личностный потенциал" [16], рассматривая его как систему ресурсов личности, которые и определяют ее возможности. Ресурсы личности могут реализовываться в разных направлениях, но в соответствии с законом сохранения энергии существует предел ее потенциала, тогда рост достижений в одном значимом направлении может привести к их снижению в других, что вызывает включение механизма обратной связи и заставляет личность перестроить свое поведение. Оптимум соответствует такой конфигурации уровней реализации потенциала по всем базовым направлениям, когда личность реализует свои наиболее значимые мотивы и у нее отсутствуют направления, по которым потенциал реализуется на слишком низком уровне. По мнению автора, достижение такого оптимума может трактоваться как акме личности.

Данная идея кажется весьма продуктивной и применимой к пониманию потенциала

организации как коллективного субъекта профессиональной деятельности. Действительно, каждый конкретный момент времени корпоративная безопасность организации определяется некоторой численной величиной, находящейся в интервале 0 - 1. Абсолютно безопасное состояние организации - иллюзия, недостижимое совершенство, крайне изменчивое и нестабильное состояние организационной системы.

Понятно, что весь жизненный цикл организации предполагает колебание в зоне измерения 0 - 1; однако практика показывает, что согласно кривой нормального распределения некоторые организации больший период времени оказываются вблизи нуля, а другие - близко к единице. Почему происходит так? Срабатывает целый ряд факторов, немаловажное значение имеет именно потенциал корпоративной безопасности, ведь ее основными целями являются ограждение ее собственности и работников от внутренних и внешних угроз, выявление и, по возможности, устранение причин их возникновения (И.А. Бородин, 2004).

Словарь управления персоналом. Корпоративная безопасность - высшее, профессионально организованное состояние социальной системы (фирмы, организации, корпорации), при котором вероятность актуализации опасности, содержащейся в факторах угрозы, минимизирована.

Разделение системы кадровой безопасности на две подсистемы продиктовано, прежде всего, тем, что на объект одновременно воздействуют два вида деструктивных сил - внешние и внутренние.

1. Внешние угрозы, к которым относятся:

- деятельность недобросовестных конкурентов, направленная на под-рыв деловой репутации организации, хищения принадлежащих ей ноу-хау, коммерческой тайны;

- действия рейдерских компаний или отдельных лиц, направленные на перехват управления организации или на захват ее имущества;

- гринмейл (greenmail, производное от green - "деньги" и blackmail - "шантаж"), то есть корпоративный шантаж в отношении организации;

- действия физических лиц из личной неприязни к юридическому лицу, его руководителям или сотрудникам, направленные на причинение ущерба материальным ценностям общества или его деловой репутации;

- неправомерные действия работников государственных силовых органов и т.д.

2. К внутренним угрозам мы относим:

- нарушения работниками трудовой дисциплины;

- правонарушения работников, направленные на причинение матери-ального ущерба организации или подрыв ее деловой репутации;

- напряжения, возникающие внутри команды из-за неправильных взаимоотношений по вертикали, горизонтали, неудовлетворенности результатами своего труда и его оценкой со стороны руководства;

- недостаточную управленческую компетентность менеджеров различного уровня;

- нездоровую конкуренцию между отдельными сотрудниками или подразделениями и др.

Специалисты указывают, что если к наличию внешних факторов угрозы отношение в целом серьезное, то внутренние факторы зачастую совсем не учитываются, хотя они обладают не меньшим, а в ряде случаев даже большим деструктивным воздействием [3].

Основными свойствами любой системы являются ее устойчивость, надежность и стабильность. В организации все три свойства детерминированы человеческим фактором. Именно он является наиболее уязвимым, наименее предсказуемым, и следовательно, он в конечном итоге определяет степень безопасности всей системы.

Вопрос 2. УСЛОВИЯ ПОВЫШЕНИЯ ПОТЕНЦИАЛА КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

С точки зрения акмеологии, обеспечение потенциала корпоративной безопасности организации от воздействия угроз может быть обусловлено усилиями менеджмента, направленными на достижение такого вершинного состояния организации, при котором актуализация угроз не будет представлять опасности; фактически это идеальное стояние и может быть метафорически представлено как "акме корпоративной безопасности организации".

Словарь управления персоналом. Акмеология - наука, возникшая на стыке естественных, общественных и гуманитарных дисциплин и изучающая закономерности и феномены развития человека до ступени его зрелости и особенно при достижении им наиболее высокого уровня в этом развитии (А.А. Бодалев, А.А. Деркач, Н.В. Кузьмина). Акмеология изучает развивающегося человека как индивида, субъекта труда и личность. У истоков формирования акмеологических идей в науке стояли выдающиеся русские ученые Б.Г. Ананьев, В.М. Бехтерев и Н.А. Рыбников, предложивший само понятие "акмеология". В настоящее время в силу гетерохронности развития акмеологического знания наибольший импульс получили исследования развития человека как субъекта труда, общих и частных закономерностей и феноменов развития профессионализма личности и деятельности, поэтому на данном этапе акмеология выступает прежде всего как наука о профессионализме. Расширение объектного и предметного полей акмеологии позволит ей обрести содержание, соответствующее заложенным при ее создании идеям.

Неудивительно, что компании, как и создавшие их люди, стремятся к стабильности, уверенности и устойчивости. Под устойчивостью функционирования объектов понимают их способность работать в нештатных, т.е. чрезвычайных ситуациях, а при нарушениях их работы - это способность восстанавливать работоспособность в кратчайшие сроки [9]. Значит, устойчивость, надежность и стабильность организационной системы достигаются за счет приобретения гибкости, мобильности и маневренности. Можно предположить, что для организации как коллективного

субъекта будет свойственна определенная зональность в пространстве ее жизнедеятельности (аналогично индивидуальному субъекту). Зона комфорта - область организационного пространства, дающая ощущение комфорта и безопасности. Как правило, зона комфорта определяется привычными шаблонами организационного поведения, регламентами, правилами, стереотипами.

Любое научение и обучение связано с выходом за границы зоны комфорта. За пределами зоны комфорта находится зона риска. В этой зоне возникает состояние дискомфорта; профессионалы констатируют, что выход в зону риска вызывает сопротивление, напряженность, конфликты и бунты у персонала [19]. Однако разумный выход в зону риска и расширение зоны комфорта за счет овладения новыми компетенциями - необходимое условие развития субъекта профессиональной организационной деятельности. Потому можно предположить, что умение действовать в зоне риска, обнаруживая и "прокачивая" эффективные и адекватные способы действий, - организационный, управленческий навык, необходимый для отреагирования в ситуации актуализации угрозы корпоративной безопасности. Здесь выпукло проявляется действие потенциала корпоративной безопасности как проявленной способности противостоять деструктивным силам без нарушения продуктивности организации.

Если менеджмент организации надолго задерживается в зоне комфорта и не предпринимает никаких усилий, чтобы выходить из этой зоны и расширять ее границы, то его развитие прекращается, постепенно переходя в фазы деградации (И. Адизес).

Развивающаяся организация, менеджмент, для которого развитие - норма организационной жизни, легко осваивает новые деятельности и выходит за границы зоны комфорта, наращивая потенциал корпоративной безопасности организации. Иными словами, чем более сформирован потенциал корпоративной безопасности организации, тем устойчивей, эффективней организация.

Определим теперь те условия, при которых увеличивается потенциал корпоративной безопасности организации.

Во-первых, отметим наличие полярно различных стилей организаци-онного управления: проактивного и реактивного. Разница между этими стилями видна из названия: цель первого - реагировать на инциденты и не допускать их повторения; цель второго - предотвращать их возникновение. Речь идет о поиске "узких мест" и скрытых ошибок в организации и ее деятельности, которые до поры никак себя не проявляют. Таким образом, речь идет о превентивных мерах управления событиями, которые желательны или нежелательны для организации. Оба стиля управления наращивают потенциал корпоративной безопасности организации, однако существенна разница в содержании: при реактивном управлении велика вероятность неадекватной реакции на возникшую угрозу, что может фактически погубить организацию; при проактивном - вероятность значительно ниже.

При всей привлекательности идеи предотвращения всех инцидентов до их возникновения нужно понимать, что это невозможно, да и неоправданно с точки зрения ресурсов. Всегда найдутся инциденты, которые дешевле устранить по факту, чем предотвращать. Поэтому необходимо поддерживать разумный баланс между проактивными и реактивными мерами. Полезно для поиска этого баланса использовать принцип Парето: 20% инцидентов приводит к 80% ущерба. Выделение

именно этих 20% и проактивное управление ими обеспечивают корпоративную безопасность организации (технологии риск-менеджмента).

Во-вторых, необходимо расширять границы организационного ком-форта. Удобно работать на основе однажды установленных правил, твердых политик, на которые можно положиться, и организационных методов, основанных на традициях.

С каждым днем подобный тип безопасной предсказуемой культуры менеджмента устаревает все больше. Эта попытка удержаться в зоне комфорта, постоянно делая стереотипные действия, абсолютно неконструктивна в глобальном, сверхконкурентном мире бизнеса XXI в., где однообразие - верный путь к стагнации, гибели. Готовность к переменам, мобильность организации, инновационный менеджмент - необходимые, а не желательные требования к организации.

Расширение границ зоны комфорта предполагает три этапа: 1) осознание границы зоны комфорта; 2) пограничное состояние (нахождение у границы); 3) расширение зоны комфорта с захватом нового пространства на поле возможностей.

Внедрять инновации, чтобы сохранять конкурентоспособность и корпоративную безопасность, - девиз сегодняшнего дня. Творчество, самообучение, развитие готовности к инновациям считается основной областью компетенции для процветающих организаций [21]. Новые продукты, новые услуги, новые модели управления - вот путь к росту. Подвижность, гибкость и быстрота реакции на требования клиентов и рынков являются отличительными характеристиками ведущих мировых организаций.

В-третьих, главным ресурсом организации исследователи единодушно признают человеческий ресурс [3, 11, 18]. Следовательно, особенности этого ресурса и составляют опору потенциала корпоративной безопасности. Адаптивность и жизнеспособность организации в ситуации неопределенности обеспечиваются рядом социально-психологических факторов. Обнаруживается целый ряд категорий, имеющих социально-психологическую природу, которые детерминируют отношение сотрудников к организации, труду, профессии, работе в целом.

Расставим эти категории в порядке обеспечения потенциала корпоративной безопасности организации. Важнейшая категория - адекватный социально-психологический климат в коллективе сотрудников, имеющий в своей основе сплоченность как интегративный эффект корпоративного самосознания персонала. Он повышает осознанность своей трудовой позиции, формирование "сильного "мы" компании и вызывает ощущение групповой социальной ответственности. И наоборот: наиболее явные угрозы корпоративной безопасности также сконцентрированы в зоне коммуникативного поля при взаимодействии сотрудников. Посмотрим далее "вглубь": под социально-психологическим климатом обнаруживается лояльность персонала, которая, в свою очередь, базируется на приверженности.

Приверженность имеет три составляющие: 1) вера в корпоративные ценности и принятие целей данной организации; 2) вовлеченность в работу, желание прилагать максимальные усилия в интересах данной организации; 3) лояльное отношение к организации, желание оставаться членом данной организации.

Все три составляющие приверженности усиливаются, если работника удовлетворяют условия его труда и перспектива профессионального роста, когда он встречает в

компании справедливое признание своих заслуг и видит возможности профессионального или должностного роста. Приверженность персонала растет, сотрудники начинают работать лучше, если у них есть внутренние обязательства перед компанией, если они понимают и принимают цели и задачи бизнеса. Таким образом, неравнодушное отношение к проблемам своей компании, готовность внести свой вклад в ее развитие и решение ее проблем основаны на ясном понимании работником целей и направления развития компании и на сближении его собственных интересов с ее интересами.

Если же организация не предпринимает целенаправленных усилий по формированию приверженности у своих работников, тогда одним рычагом воздействия на мотивацию персонала становится меньше. В основе приверженности лежат два полюса: ценности человека, конгруэнтные ценностям организации, и связанное с этим доверие к организации.

Корпоративные ценности лежат в основе отношения человека и организации и выступают кристаллизированной сущностью корпоративной культуры и безопасности организации. Эти ценности постепенно присваиваются вновь инкорпорированными сотрудниками, а старожилы организации являются их носителями и приверженцами. Стоит предположить, что их личные ценности согласованы с корпоративными - потому они и "органичны организации". Присвоение ценностей формирует феномен организационной идентичности сотрудника. Предназначение и основная функция корпоративных ценностей состоят в контроле и регулировании корпоративного сознания и поведения человека в организации [25]. Вместе это приводит к формированию социальной корпоративной ответственности персонала, которая и обеспечивает социально-психологический фундамент потенциала корпоративной безопасности.

Каждая организация в процессе становления, развития и функционирования обретает специфическую ценностно-нормативную систему, соответствующую своим целям, учитывающую организационные и корпоративные ценности. Именно ценности, разделяемые и декларируемые основателями и наиболее авторитетными членами организации, зачастую становятся тем ключевым звеном, от которого зависит сплоченность сотрудников различных подразделений и уровней управления, формируется единство взглядов и действий, а следовательно, обеспечивается эффективное достижение целей организации. Речь идет о центральной корпоративной системе ценностей, которая является слоем, объединяющим внутренние и внешние среды, а также нижние и верхние уровни управления. В ней объединяются интересы всех участников деятельности: руководства, сотрудников и акционеров. В организациях, ориентированных на клиента, в корпоративной системе ценностей присутствуют интересы клиентов.

Разделяя и развивая взгляды современного отечественного психолога Д.А. Леонтьева, можно выделить три основные формы, или стадии динамики существования корпоративных ценностей:

1) идеалы - выработанные руководством и разделяемые им обобщенные представления о совершенстве в различных проявлениях и сферах деятельности организации;

2) воплощение этих идеалов в деятельности и поведении сотрудников в рамках

организации;

3) внутренние мотивационные структуры личности сотрудников организации, побуждающие к воплощению в своем поведении и деятельности корпоративных ценностных идеалов.

Эти формы имеют иерархическую структуру осознания работниками и постепенно переходят одна в другую: организационно-культурные идеалы усваиваются сотрудниками и начинают побуждать их активность в качестве "моделей должного", в результате чего происходит предметное воплощение этих моделей. Предметно воплощенные ценности, в свою очередь, становятся основой для формирования организационных идеалов и так далее до бесконечности. Этот процесс повторяется, непрерывно совершенствуясь на каждом новом витке развития корпоративной культуры организации.

Организационная идентичность позитивно влияет на результаты работы коллектива. Она повышает кооперацию, старания, вовлеченность, приверженность, взаимовыручку и поддержку между членами коллектива [4].

Организационная идентичность позитивно влияет на принятие решений, выгодных для организации. Особенно многообещающими в контексте нашей тематики являются результаты исследований, которые показали, что индивид, действующий как микрокосмос организации, способен на пожертвование своими личными интересами во имя организации [14].

Наши исследования показывают, что с точки зрения потенциала корпоративной безопасности в центре внимания все чаще оказывается не столько индивид, личность, сколько "человеческий ресурс", "коллективный субъект", группа в совокупности внутренних и внешних связей. Для обеспечения корпоративной безопасности важна интеграция человека и организации, своеобразное "вмонтирование" человека в "самость организации", при том роль специалиста, менеджера внутри организации все чаще сводится к своевременному и точному выполнению функциональных обязанностей, определяемых менеджментом более высокого звена, который, в свою очередь, является проводником видения первых лиц организации. Работа требует, как правило, частичного или почти полного отказа человека от своего индивидуального "я" в пользу коллективного "я" в интересах получения группой положительного результата, который во все большей степени понимается как продажа вещественного результата деятельности на рынке. Только после этого индивид может через процессы распределения и перераспределения получить свою личную долю в обезличенном сертификате его вклада в реализованный продукт - деньгах. Этот механизм действительно обеспечивает устойчивость, корпоративную безопасность организации.

Реализация этого механизма в организации предлагает человеку жизнь по чужому сценарию не только как социально поощряемую культурную норму, но и как оптимальную жизненную стратегию. Возникает вопрос: а возможно ли в этих условиях достижение акме самого человека, его личности, профессионализма? Заинтересована ли организация в создании условий для самоактуализации персонала? Наши исследования показывают, что потенциал корпоративной безопасности организации и акме человека отрицательно коррелируют между собой. Однако в рамках тематики этой статьи этот результат является побочным.

Вывод: рассматривая акмеологический потенциал корпоративной безопасности организации, отметим, что этот необходимый для продуктивной организационно-профессиональной деятельности конструкт имеет сложную иерархическую структуру, связан с социально-психологическими, управленческими, собственно акмеологическими характеристиками самой организации и персонала и фактически является сложно диагностируемым, экзистенциальным фундаментом самого существования любой организации.

Библиография

1. Акмеология: Учеб. Изд. 2-е, перераб. / Под общ. ред. А.А. Деркача. М.: РАГС, 2006.

2. Байков Н.М. Кадровый потенциал органов государственной власти и муниципального управления (социологический анализ). Докт. дис. М., 2002.

3. Бородин И.А. Психология корпоративной безопасности. М.: Высшая школа психологии, 2004.

4. Ван Дик Р. Преданность и идентификация в организации. Харьков: Гуманитарный Центр, 2006.

5. Галль Ж.М. Управление людскими ресурсами. М.: Инфра-М, 1995.

6. Гладышевский А.И. Формирование производственного потенциала: анализ и прогнозирование. М.: Наука, 1992.

7. Грейсон Дж., Делл О. Американский менеджмент на пороге XXI века. М.: Экономика, 1991.

9. Криворотов В.С., Минбаева Л.Ф. Анализ и формирование механизма экономической устойчивости предприятия. М.: Пищевая промышленность, 2006.

10. Крылова Н.Б. Эстетический потенциал культуры. М.: Высшая школа, 1990.

11. Лобанов А.А. Человеческие ресурсы. М.: Дело, 1993.

12. Ладанов И.Д. Практический менеджмент (психотехника управления и самотренировки). М.: Элник, 1995.

13. Лавизина О.В. Некоторые аспекты управления жизненным циклом организации, понимаемой как социальная система // Менеджмент в России и за рубежом. 2003. N 5.

14. Липатов С.А. Социальная идентичность работников в организационных условиях // Идентичность и организация в меняющемся мире: Сб. науч. ст. / Под ред. Н.М. Лебедевой, Н.Л. Ивановой, В.А. Штроо. М.: Изд. дом ГУ-ВШЭ, 2008.

15. Магура М.И. Чем, кроме денег, можно мотивировать персонал? // [Электронный ресурс] Режим доступа: http://www.gkmim.ru/index. php?area=publication&pub=9.5.

16. Марков В.Н. Личностно-профессиональный потенциал кадров управления: психолого-акмеологическая оценка и оптимизация. Автореф. дис. ... д-ра психол. наук. М.: 2004.

17. Мерцалов А.А. Трудовой потенциал российской молодежи: структура, воспроизводство, перспективы. М.: Луч, 1992.

18. Одегов Ю.Г., Журавлев П.В. Управление персоналом. М.: Финстагинформ, 1997.

19. Панова Т.В. Как преодолеть сопротивление персонала // Генеральный директор. 2007. N 4.

20. Селезнев А.М. Научный потенциал современного общества. М.: Изд-во МГУ, 1989.

21. Сенге П. Пятая дисциплина: искусство и практика самообучающейся организации. М.: Олимп-Бизнес, 1999.

22. Управление человеческими ресурсами в японских компаниях (информационно-аналитическая разработка Минтруда России). Москва - Казань: Таглимат ИЭУП, 1995.

23. Управление персоналом: Учеб. / Под общ. ред. А.И. Турчинова. М.: РАГС, 2002.

24. Хучек М. Стратегия управления трудовым потенциалом предприятия. М.: РАУ, 1993.

25. Харский К.В. Благонадежность и лояльность персонала. СПб.: ПИТЕР, 2007.

ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Практическое занятие 1

КАДРОВАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Учебные вопросы:

1. Сущность видов безопасности.
2. Основные принципы обеспечения кадровой безопасности организации.

Вопрос 1. СУЩНОСТЬ ВИДОВ БЕЗОПАСНОСТИ

Безопасность организации - это такое состояние, которое достигается посредством обеспечения и поддержания защищенности ее персонала и жизненно важных интересов организации от внутренних и внешних угроз с целью уменьшения отрицательных последствий нежелательных событий и достижения наилучших результатов деятельности.

Угроза безопасности организации - это событие, действие или явление, которое посредством воздействия на персонал, финансовые, материальные ценности и информацию может привести к нанесению вреда здоровью работников и ущерба организации, нарушению или приостановке ее функционирования.

Обеспечение безопасности организации - это деятельность ее должностных лиц, персонала, специального подразделения по безопасности, государственных правоохранительных органов и иных структур, направленная на предотвращение возможного нарушения ее нормального функционирования.

Система безопасности организации - это комплекс организационно-управленческих, экономических, правовых, социально-психологических, профилактических, пропагандистских, режимных и инженерно-технических мер и мероприятий, направленных на обеспечение безопасности организации и ее персонала. Определяющим и изначальным при формировании системы безопасности является концепция безопасности организации, которая представляет собой свод основных документов, касающихся политики и стратегии безопасности, основных направлений, средств и методов ее обеспечения.

Рассмотрим сущность видов безопасности.

Физическая безопасность объекта - это охрана материальных и финансовых ресурсов от чрезвычайных обстоятельств (пожар, стихийное бедствие, терроризм) и от несанкционированного проникновения на территорию (вандализм, кража, хищение и т.д.). Обеспечение безопасности объектов регулируется Законом РФ от 11.03.1992 N

2487-1 "О частной детективной и охранной деятельности в Российской Федерации" (ред. от 27.12.2009), положениями и инструкциями, разрабатываемыми и вводимыми в действие Службой государственного пожарного надзора и Управления вневедомственной охраны МВД России.

Этот вид безопасности объекта обеспечивается деятельностью сотрудников службы охраны путем соблюдения пропускного объектового и внутриобъектового режимов с применением соответствующих охранных технических средств и систем. К техническим и инженерно-техническим охранным средствам и системам относятся: периметральные охранные системы; системы охранной сигнализации; системы пожарной сигнализации, пожаротушения и оповещения; системы охранного телевидения; системы ограничения доступа; системы управления доступом; средства оперативной связи; защитные инженерные средства (решетки, жалюзи, бронестекла и др.).

Физическая безопасность персонала подразделяется на личную безопасность руководства и ведущих специалистов и безопасность всего персонала в целом.

Личная безопасность руководства и ведущих специалистов - это их физическая охрана, а также охрана жилья и средств передвижения руководителей и ведущих специалистов организации и членов их семей. Личная безопасность обеспечивается целым комплексом оперативных и технических мер по охране лица как в обычных повседневных, так и экстремальных условиях. Проведение мероприятий по обеспечению личной безопасности охраняемого лица регулируется Законом РФ "О частной детективной и охранной деятельности".

Физическая безопасность персонала - это система охраны труда и техники безопасности в организации на основе производственной санитарии и психологии деловых отношений. Безопасные и здоровые условия труда в организации обеспечиваются комплексным взаимодействием как руководства организации, так и, не в последнюю очередь, усилиями самого персонала организации. Системы охраны труда и техники безопасности в организации регламентируются Трудовым кодексом РФ (разд. X), Законом РФ "Об основах охраны труда в Российской Федерации" и нормативными правовыми актами по охране труда.

Экономическая безопасность - это состояние защищенности экономических интересов организации от внутренних и внешних угроз посредством минимизации коммерческих рисков, системы мер экономического, правового и организационного характера, разработанной администрацией организации. Экономическая безопасность характеризуется совокупностью качественных и количественных показателей и включает в себя следующие функциональные составляющие: финансовую, имущественную, валютную, кредитную, политико-правовую и др. Экономическая безопасность выступает материальной основой решения практически всех задач, связанных с функционированием организации.

Информационная безопасность - это охрана каналов поступления, хранения, обработки и передачи информации, защита любых информационных ресурсов по уровням доступа. Защите подлежит любая документационная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты информации устанавливается в отношении конфиденциальной документационной информации собственником

информационных ресурсов, т.е. самой организацией.

Результатами реализации угроз информации могут быть: утрата (разрушение, уничтожение), утечка (извлечение, копирование, подслушивание), искажение (модификация, подделка), блокирование.

Существует два основных принципа защиты информации: разделение обязанностей и минимизация привилегий. Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не смог нарушить критически важный для предприятия процесс. Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. При этом высокий уровень информационной безопасности организации обеспечивается целым комплексом административных мер и оперативно-технических мероприятий.

Юридическая безопасность - это охрана прав, порядка и условий осуществления конкурентной предпринимательской деятельности организации в рамках законодательства Российской Федерации. Если рассматривать юридическую защиту более подробно, то условно ее можно подразделить на три основных направления:

- взаимоотношения с органами государственной власти;

- защита от действий недобросовестных партнеров, заказчиков или контрагентов;

- создание условий для успешной производственной деятельности организации.

Интеллектуальная безопасность - охрана прав на научные труды, промышленные образцы, товарные знаки, коммерческие наименования. На основе Гражданского кодекса РФ (ст. 138) "признается исключительное право (интеллектуальная собственность)... юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации. Использование результатов интеллектуальной деятельности и средств индивидуализации может осуществляться третьими лицами только с согласия правообладателя".

Экологическая безопасность - охрана окружающей среды, обеспечение безопасной работы экологически опасных объектов предприятия, предотвращение экологических катастроф. В общем виде вопросы экологической безопасности организаций регулируются соответствующими законами Российской Федерации. Экологическая составляющая безопасности в структуре безопасности предприятия является достаточно специфичным явлением и в основном значимо для предприятий, имеющих экологически опасные производства или занимающихся разработкой недр и т.д.

И наконец, кадровая безопасность - это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом.

Виды угроз со стороны персонала:

1. Хищение имущества предприятия.

2. Использование ресурсов предприятия в собственных целях.

3. Умышленная порча и уничтожение имущества предприятия.

4. Получение заработной платы за невыполняемую работу.

5. Шантаж компетентностью (я - незаменимый работник).

6. Шантаж полномочиями (концентрация полномочий в одних руках).

7. Торговля коммерческими секретами.

8. Дисциплинарные нарушения.

9. Создание в коллективе невыносимого морально-психологического климата.

Очевидно, что кадровая безопасность занимает доминирующее положение по отношению к другим элементам системы безопасности организации, так как она имеет дело с персоналом, который в любой составляющей первичен.

Статистика ущерба.

Около 80% ущерба материальным активам компаний наносится их собственным персоналом. Только 20% попыток взлома сетей и получения несанкционированного доступа к компьютерной информации приходит извне. Остальные 80% случаев спровоцированы с участием персонала компаний.

Также невозможно обойти вниманием и общемировую статистику, применимую и к России: 10 - 15% всех людей являются нечестными по определению, 10 - 15% абсолютно честные, остальные 70 - 80% - колеблющиеся, то есть те, кто поступит нечестно, если риск попасться будет минимальным.

Еще немного американской статистики. Стоимость преступлений, со-вершенных должностными лицами и работниками американских компаний, в 1980 г. составила 50 млрд долл. США, в 1990 - 250 млрд долл. США, в 1998 - 400 млрд долл. США, в 2008 - 600 млрд долл. США.

Последняя цифра означает, что каждый работник каждой американской организации (в исследовании участвуют частные и государственные учреждения и предприятия) крадет у своего работодателя больше 12 долл. США в день круглый год.

Мошенничество сотрудников стало основной причиной вынужденного закрытия около 100 американских банков за последние 20 лет. 95% ущерба, понесенного в банковской сфере США, образуется при непосредственном участии персонала банков и только 5% - за счет действий клиентов и иных лиц.

Субъектом кадровой безопасности является служба управления персоналом, причем вопросы кадровой безопасности должны решаться на каждом этапе управления персоналом (поиск, отбор, прием, адаптация, развитие, оценка и т.д.). Любое действие менеджера по персоналу на любом этапе - это либо усиление, либо ослабление безопасности компании по главной ее составляющей - по персоналу.

Вопрос 2. ОСНОВНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Как показывает практический опыт, обеспечение безопасности организации должно соответствовать следующим принципам:

- непрерывность - осуществление мер по обеспечению безопасности должно быть основано на постоянной готовности к отражению как внутренних, так и внешних угроз безопасности организации. При этом руководители организаций должны ясно осознавать: процесс обеспечения безопасности не допускает перерывов, иначе придется все начинать сначала;

- комплексность - использование всех средств защиты финансовых, материальных, информационных и человеческих ресурсов во всех структурных подразделениях организации и на всех этапах ее деятельности. При этом комплексность реализуется через совокупность правовых, организационных и инженерно-технических мероприятий без их приоритетного выделения;

- своевременность - обеспечение безопасности с использованием упреждающих мер. При этом принцип своевременности предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности, а также разработку эффективных мер предупреждения посягательств на интересы организации;

- законность - обеспечение безопасности на основе законодательства РФ и других нормативных актов, утвержденных органами государственного управления в пределах их компетенции. При этом необходимо иметь в виду, что вопрос дозволенности тех или иных методов обнаружения и пресечения правонарушений в рамках действующего законодательства и большого количества ведомственных подзаконных актов в настоящее время в большинстве случаев остается открытым;

- активность - обеспечение безопасности организации с достаточной степенью настойчивости и с широким использованием маневра имеющихся сил и средств;

- универсальность - обеспечение безопасности посредством применения таких мер и проведения таких мероприятий, которые дают положительный эффект независимо от места их конкретного применения;

- экономическая целесообразность - сопоставление возможного ущерба и затрат на обеспечение безопасности. При этом во всех случаях стоимость системы безопасности должна не превышать размера возможного ущерба от любых видов риска;

- конкретность и надежность - определение конкретных видов ресурсов, выделяемых на обеспечение безопасности. При этом обязательным является достаточное дублирование методов, средств и форм защиты при обеспечении безопасности организации;

- профессионализм - реализация мер безопасности должна осуществляться только профессионально подготовленными специалистами. При этом в условиях быстрого развития средств и систем безопасности необходимо постоянное совершенствование мер и средств защиты на базе обучения личного состава;

- взаимодействие и координация - осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений, служб и ответственных лиц. При этом вопрос о взаимодействии и координации касается не только подразделений и лиц, непосредственно отвечающих за безопасность, но и их связи с остальными подразделениями организации;

- централизация управления и автономность - обеспечение организационно-функциональной самостоятельности процесса организации защиты всех объектов охраны и централизованное управление обеспечением безопасности организации в целом.

Тесно связана с кадровой безопасностью безопасность труда и здоровья персонала - система обеспечения безопасности жизни и здоровья работников в процессе трудовой деятельности, включающая правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия (ст. 1 Основ законодательства РФ об охране труда).

Безопасность организации обеспечивается посредством взаимодействия администрации, подразделения охраны труда и техники безопасности и самого работника. С этой целью в организациях разрабатываются комплексные планы организационно-технических, социально-экономических и психологических мероприятий по обеспечению безопасности организации.

Основой для разработки таких планов может послужить построение "дерева целей" системы безопасности организации. На рис. 1 приведен фрагмент "дерева целей" системы безопасности организации на примере одного из важнейших направлений безопасности - кадровой безопасности организации.

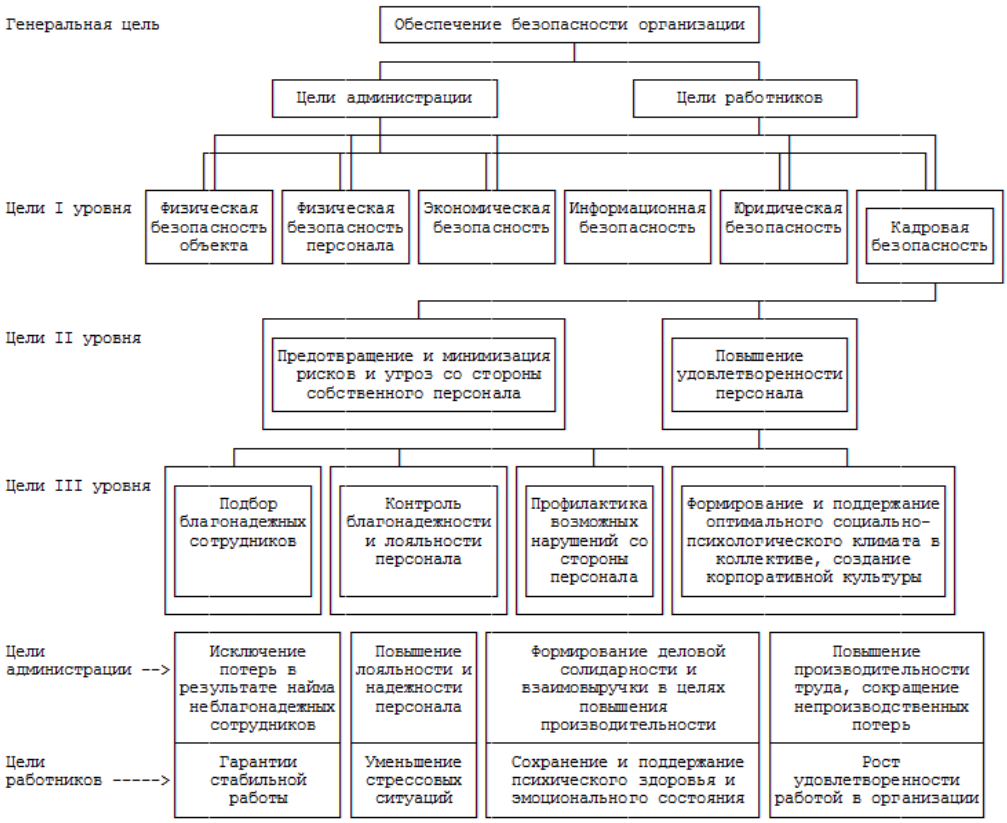


Рис. 1 Дерево целей

Библиография

1. Бадалова А.Г., Москвитин К.П. Управление кадровыми рисками предприятия // Российское предпринимательство. 2005. N 7.

2. Управление персоналом организации: Учеб. / Под ред. А.Я. Кибанова. М.: ИНФРА-М, 2006.

Практическое занятие 2

МЕТОДИКА ОЦЕНКИ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ ФИРМЫ

Учебные вопросы:

1. Тестирование плана ОНиВД как способ выявления угроз безопасности фирмы.
2. Обеспечение информационной безопасности фирмы.
3. Составление вопросника для аудита системы безопасности фирмы в рамках ОНиВД

Введение

Ключевым вопросом системы обеспечения непрерывности деятельности фирмы является обеспечение безопасности ее персонала и активов - причем как материальных, так и нематериальных - при чрезвычайном происшествии. В сущности, на реализацию этих задач и направлен план обеспечения непрерывности и восстановления деятельности (ОНиВД) фирмы.

В каждой инструкции, в каждом плане ОНиВД по отдельным бизнес-процессам (информационные технологии, безопасность, противодействие отмыванию доходов и финансированию терроризма и т.д.) и на случай наступления чрезвычайных происшествий (пожар, террористический акт, наводнение и т.д.), входящих в систему документов по обеспечению непрерывности деятельности, первым и наиболее значимым мероприятием значится эвакуация персонала (клиентов) и важнейших документов фирмы с места происшествия, а также введение режима охраны объекта и прочие действия, направленные на обеспечение безопасности активов фирмы. От качественного набора мероприятий и порядка их проведения зависит успешность прохождения фирмой фазы кризиса и перехода к фазам восстановления и нормализации режима работы. В немалой степени это зависит от наличия регламента взаимодействия служб фирмы, несущих непосредственную ответственность за обеспечение безопасности. Очевидно, что разработка такого регламента, равно как и системы мер обеспечения непрерывности деятельности фирмы, возможна только во взаимодействии с этими службами.

Так, подразделение информационных технологий несет ответственность за защиту и восстановление информационных систем и баз данных, создание соответствующей инфраструктуры и телекоммуникаций. Административно-хозяйственный департамент ответственен за физическое состояние оборудования фирмы, департамент безопасности - за обеспечение безопасности активов фирмы в целом, охрану персонала и территории. Подразделение по работе с персоналом ведет учет кадрового состава и обеспечивает возможность замещения ключевых позиций при чрезвычайном происшествии. Руководители бизнес-подразделений - в рамках их компетенции - ответственны за оперативное внедрение операций по направлению деятельности фирмы.

Задача службы внутреннего контроля в процессе обеспечения безопасности

заключается в том, чтобы, во-первых, дать адекватную оценку качества системы планов ОНиВД с точки зрения охвата ею всех возможных угроз безопасности активов фирмы, а во-вторых, оценить возможности реализации плана ОНиВД и восстановления деятельности фирмы после наступления чрезвычайной ситуации. Иными словами, сотрудники службы внутреннего контроля выступают в данном случае в роли комплекс-контролеров системы обеспечения непрерывности деятельности фирмы. Основным инструментом реализации обозначенных задач внутреннего контроля является проведение аудита и тестирования документов ОНиВД. Используемая при этом методика - формирование базы вопросников для оценки эффективности всех мероприятий обеспечения безопасности фирмы в случае чрезвычайного происшествия.

Вопрос 1. ТЕСТИРОВАНИЕ ПЛАНА ОНиВД КАК СПОСОБ ВЫЯВЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ФИРМЫ

Единственным, по сути, способом проверки эффективности мер по обеспечению безопасности деятельности фирмы в случае чрезвычайного происшествия является проведение тестирования, причем в виде полноценных учений.

Необходимо провести хотя бы одну фактическую проверку плана ОНиВД, чтобы удостовериться, что персонал компании осознает свою роль и понимает порядок своих действий при возникновении кризисной ситуации, слаженно работают подразделения фирмы, обеспечивается безопасность активов фирмы и персонала при разработанном порядке мероприятий по обеспечению непрерывности и восстановлению деятельности фирмы. При такой проверке у каждого подразделения - участника реализации плана ОНиВД есть шанс получить наиболее полное представление о том, что же надо усовершенствовать. Уровень стресса среди участников тестирования при проведении такой проверки, конечно же, ниже, чем при реальном чрезвычайном происшествии. Практические проверки способствуют устранению ошибок в разработке плана, совершенствованию процедур, а также дают возможность оценить взаимодействие компонентов плана ОНиВД.

Тестирование плана ОНиВД, как правило, координирует подразделение внутреннего контроля, которое собирает руководителей ответственных подразделений - участников рабочих групп по обеспечению непрерывности деятельности фирмы. В группу тестирования плана ОНиВД входят представители департамента управления рисками, административно-хозяйственного департамента, департамента безопасности, подразделения по работе с персоналом, подразделения информационных технологий, собственно службы внутреннего контроля и, при необходимости, представители других подразделений фирмы.

Группа тестирования плана ОНиВД разрабатывает программу тестирования, которая включает сценарии учений и испытаний, распределение обязанностей между представителями подразделений в части проведения учений и испытаний, шкалу оценки результатов. В программу тестирования включаются следующие разделы:

- подробное описание всех этапов теста с указанием целей и задач;

- распределение ролей и обязанностей ответственных участников тестирования;

- круг участников тестирования;

- объекты тестирования;

- условия тестирования;

- арбитры тестирования и порядок выставления оценок жизнеспособности плана ОНиВД.

Существует определенная последовательность действий при наступлении того или иного чрезвычайного события. При разработке программы тестирования, а также его реализации проверяются качество выполнения этих мероприятий и обеспечение при этом безопасности сотрудников фирмы, а также оборудования и информации.

К примеру, при пожаре должны быть предприняты следующие действия:

- тушение огнетушителями и с использованием иных специальных средств;

- эвакуация сотрудников, важнейших документов, копирование и передача в хранилище баз данных;

- вызов службы тушения пожара;

- отключение всех систем и оборудования;

- учет количества сотрудников и поиск пропавших.

За реализацию каждого из обозначенных мероприятий ответственно конкретное подразделение, которое действует по четко разработанному плану. Так, подразделение безопасности организует мероприятия по усилению охраны, обеспечению пропускного и внутриобъектового режимов в зданиях фирмы, охране ценностей и выносимого имущества в местах его сосредоточения и массового скопления людей. Административно-хозяйственное подразделение организует освобождение подъездных и эвакуационных путей к объектам фирмы, проводит эвакуацию работников с объекта согласно плану эвакуации, взаимодействует с формированиями МЧС, прибывающими для тушения пожара, а также с формированиями, которые смогут прибыть с соседних объектов для оказания помощи в тушении пожара.

Работники фирмы при поступлении сигнала (команды) об эвакуации должны отключить от электропитания оргтехнику и другое оборудование, находящееся в рабочих помещениях, взять личные вещи, закрыть двери и окна рабочего помещения, одновременно с тушением пожара организовать эвакуацию и защиту документов и материальных ценностей, не пользуясь при этом лифтами.

После осуществления эвакуационных мероприятий кадровая служба организует вне здания перекличку персонала по подразделениям, устанавливает работников, оставшихся в помещениях, и докладывает об этом руководителю подразделения фирмы, который, в свою очередь, отчитывается перед руководством фирмы.

Слаженность работы всех служб фирмы при выполнении обозначенных действий в случае пожара должна обеспечить наибольшую степень безопасности сотрудников

фирмы и ее материальных активов.

При наводнении в первую очередь выясняют причины увеличения уровня воды и оценивают угрозы персоналу и имуществу. Затем передают информацию в хранилище данных (в т.ч. резервное). В случае если угроза повышения уровня воды является очевидной, вызывают спасателей, отключают электроэнергию в офисе, в наибольшей степени подверженном опасности быть затопленным, выносят ценные документы и эвакуируют персонал фирмы. Весьма важны также учет количества сотрудников и последующий поиск пропавших.

Ураган не является частым явлением, но последствия этого природного явления могут оказать существенное влияние на непрерывность деятельности фирмы. При возникновении угрозы данного природного явления отключают оборудование от электрических сетей. В случае поступления информации о силе урагана и его опасности для жизни людей проводят эвакуацию персонала и оборудования в безопасное место.

При пожаре, наводнении, урагане и прочих природных и техногенных происшествиях возникает опасность загрязнения воздуха. При этом мерами первостепенной важности являются анализ факторов обнаружения опасности и обеспечение людей средствами защиты от загрязнения воздуха (воздушно-марлевыми повязками, респираторами). В этом случае должна быть реализована схема оперативной эвакуации людей.

Одним из наиболее частых чрезвычайных происшествий является отключение электроэнергии, которое может произойти в результате природных факторов (урагана, пожаров и т.д.), злонамеренных действий и техногенных катастроф (аварий на подстанциях). Сбои в энергообеспечении влекут за собой нарушение работы компьютерных систем, возникновение пожаров, нагревов/переохлаждения оборудования. В этом случае необходимо отключить от энергосети оборудование (компьютеры на рабочих местах), подключить резервные источники питания, информировать энергокомпанию и собственника здания (в случае если фирма арендует помещение) о факте отсутствия электроэнергии, подготовить оборудование к подключению электроэнергии. При аварии на энергоподстанции офис должен быть перенесен в резервное помещение.

И только после того, как приняты первичные меры при наступлении чрезвычайного события и обеспечена безопасность сотрудников фирмы, ее оборудования и информации, в действие вступают планы восстановления операций в соответствии с видом события.

Тестирование плана ОНиВД обычно начинается с имитационного моделирования событий, то есть рассматриваются гипотетические варианты развития событий. Каждую из потенциальных проблем обсуждают отдельно, а участники решают их путем мозгового штурма. В ходе такой своеобразной игры участники управляют фиктивным инцидентом, информационными потоками, принимают решения, протоколируют свои действия, а также учатся решать нетривиальные задачи и слаженно работать в команде.

После этого план ОНиВД необходимо протестировать в условиях, максимально приближенных к действительности, что позволяет сотрудникам внутреннего контроля наглядно убедиться в жизнеспособности планов ОНиВД фирмы. Такая проверка

должна проводиться по крайней мере ежегодно, желательно в каждом из офисов фирмы.

По окончании тестирования (причем как с использованием методов имитационного моделирования, так и при полномасштабных учениях) группа тестирования составляет отчет и дает рекомендации по корректировке плана ОНиВД.

В отчет включается такая информация, как:

- место, дата и продолжительность испытаний;

- перечень подразделений и список работников фирмы, участвовавших в испытаниях;

- описание моделируемой чрезвычайной ситуации;

- решения, принятые руководителями фирмы для ликвидации чрезвычайной ситуации;

- результаты исполнения принятых решений, а именно: полное восстановление функционирования подразделения фирмы, частичное восстановление (в какой степени) или отсутствие результатов;

- причины наступления указанных результатов;

- выявленные в ходе испытаний проблемы (подготовка работников и руководителей фирмы, структура и содержание плана ОНиВД, материально-техническое обеспечение);

- краткие выводы и рекомендации по корректировке плана ОНиВД.

Отчет подписывается всеми членами группы тестирования плана ОНиВД и руководителями подразделений фирмы, принимавших участие в данных испытаниях, после чего направляется на рассмотрение совета директоров фирмы.

Следует отметить, что затраты фирмы, связанные с организацией процедур тестирования, несоизмеримы с той экономией, которую получит фирма в случае чрезвычайного происшествия. К сожалению, этот факт не является очевидным для топ-менеджеров и акционеров российских фирм, которые в большинстве своем не учитывают потери от растерянности персонала фирмы и отсутствия слаженных действий для возобновления операций при внештатных ситуациях. Видимо, менеджерам фирмы проще списывать многомиллионные убытки от прерывания операций на пожар, ограбление, отключение электричества или другие какие-либо чрезвычайные события, чем предпринимать конкретные действия по обеспечению непрерывности деятельности до того, как эти события наступят. К тому же ответственность за халатность и отсутствие превентивных мер со стороны акционеров фирм в российской практике - явление чрезвычайно редкое.

Доведение до акционеров и совета директоров фирмы информации о значимости мер по разработке и внедрению плана ОНиВД является одной из важнейших задач службы внутреннего контроля. Тем более что именно совет директоров инициирует проведение тестирования плана ОНиВД, формирует инициативные группы, утверждает программу тестирования и т.д.

Вопрос 2. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФИРМЫ

Одной из наиболее важных угроз для непрерывности деятельности фирмы при наступлении чрезвычайного события является потеря информации или несанкционированное использование ее третьими лицами. Попросту говоря, чрезвычайное происшествие может пробить брешь в системе информационной безопасности фирмы. Поэтому важно проводить не только физическое тестирование возможностей резервирования информационной системы фирмы при возникновении чрезвычайного происшествия, но и комплексные проверки системы информационной безопасности в целом.

Самой большой проблемой при проведении таких проверок является отсутствие у персонала службы внутреннего контроля навыков и знаний в области информационных технологий. Соответственно, подготовка к такой проверке должна проводиться задолго до ее инициации.

Проверка систем информационной безопасности специалистами службы внутреннего контроля проводится поэтапно.

На первом этапе осуществляется собственно инициирование процедуры проверки, причем руководством фирмы, поддержка которого является необходимым условием. В ходе проверки оказываются задействованными представители большинства структурных подразделений фирмы. Действия всех участников этого процесса должны быть скоординированы.

На этапе инициирования процедуры проверок должны быть определены границы проведения обследования. Одни информационные подсистемы компании не являются достаточно критичными, и их можно исключить из области проведения обследования. Другие подсистемы могут оказаться недоступными для проверок из-за соображений конфиденциальности. Безусловной проверке следует подвергать информационные системы, которые должны быть задействованы в ходе реализации мер по обеспечению непрерывности деятельности фирмы.

Сотрудники службы внутреннего контроля должны составить список обследуемых физических, программных и информационных ресурсов, обозначить основные виды угроз безопасности, рассматриваемые при проведении проверки, в особенности при прерывании деятельности фирмы, а также учесть организационные (законодательные, административные и процедурные), физические, программно-технические и прочие аспекты обеспечения безопасности и их приоритеты (т.е. в каком объеме они должны быть учтены).

План и границы проведения проверки обсуждаются на рабочем собрании, в котором участвуют специалисты службы внутреннего контроля, руководство фирмы и руководители структурных подразделений.

На втором этапе необходимо собрать информацию для проверки информационной безопасности, что является наиболее сложным и длительным. Это связано с тем, что в большинстве российских фирм необходимая документация на информационную систему отсутствует, кроме того, специалист внутреннего контроля должен плотно взаимодействовать со многими должностными лицами организации.

Получение информации о текущем состоянии информационной системы осуществляется сотрудником внутреннего контроля в ходе интервью с ответственными лицами, путем изучения технической и организационно-распорядительной документации, а также исследования автоматизированной системы с использованием специализированного программного инструментария.

Обеспечение информационной безопасности организации - это комплексный процесс, требующий четкой организации и дисциплины. Он должен начинаться с определения ролей и распределения ответственности среди должностных лиц, занимающихся информационной безопасностью. Поэтому первый пункт проверки начинается с получения информации об организационной структуре пользователей информационной системы и обслуживающих ее подразделений. В связи с этим в пакет информации, запрашиваемой специалистом внутреннего контроля, как минимум должны входить схема организационной структуры пользователей и схема организационной структуры обслуживающих подразделений, а также функциональные схемы, описания автоматизированных функций, основных технических решений, другая проектная и рабочая документация на информационную систему. Кроме того, необходимо понять, каким образом будет обеспечена сохранность информации при возникновении различных чрезвычайных происшествий.

Назначение и принципы функционирования информационной системы во многом определяют существующие риски и требования безопасности, предъявляемые к системе.

Далее необходимо получить более детальную информацию о структуре автоматизированной системы (АС). Это позволит уяснить, каким образом осуществляется распределение механизмов безопасности по структурным элементам и уровням функционирования системы. Типовые вопросы, на которые должен быть получен ответ, могут быть следующими:

- из каких компонентов (подсистем) состоит информационная система;

- функциональность отдельных компонентов;

- где проходят границы системы;

- какие точки входа имеются;

- как информационная система взаимодействует с другими системами;

- какие каналы связи используются для взаимодействия с другими информационными системами;

- какие каналы связи используются для взаимодействия между компонентами системы;

- по каким протоколам осуществляется взаимодействие;

- какие программно-технические платформы используются при построении системы.

Для ответа на эти вопросы необходимо запастись такой документацией, как структурная схема информационной системы, схема информационных потоков, описание структуры комплекса технических средств информационной системы,

описание структуры программного обеспечения, описание структуры информационного обеспечения, схема размещения компонентов информационной системы.

После получения всей необходимой информации переходят к ее анализу. Используемые при этом методы определяются выбранными подходами к проведению аудита, которые могут существенно различаться.

Первый подход, самый сложный, базируется на анализе рисков. Опираясь на методы анализа рисков, сотрудник службы внутреннего контроля определяет для обследуемой АС индивидуальный набор требований безопасности, в наибольшей степени учитывающий особенности данной информационной системы, среды ее функционирования и существующие в данной среде угрозы безопасности, в особенности при реализации различных сценариев возникновения чрезвычайных происшествий. Данный подход является наиболее трудоемким и требует высокой квалификации проверяющего. На качество результатов проверки в этом случае сильно влияют используемая методология анализа и управления рисками и ее применимость к данному типу информационной системы.

Обследование безопасности АС должно определить, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам информационной системы в случае чрезвычайного происшествия.

Процесс анализа рисков можно разделить на несколько последовательных этапов:

- идентификация ключевых ресурсов информационной системы (информационные ресурсы, программное обеспечение, технические средства (серверы, рабочие станции, активное сетевое оборудование и т.п.), людские ресурсы).

Необходимо идентифицировать только те ресурсы, которые определяют функциональность информационной системы и существенны с точки зрения обеспечения безопасности;

- определение важности тех или иных ресурсов для фирмы.

Важность (или стоимость) ресурса определяется величиной ущерба, наносимого в случае нарушения конфиденциальности, целостности или доступности этого ресурса. В результате чрезвычайного происшествия нарушения в непрерывности деятельности фирмы могут быть спровоцированы раскрытием, изменением, недоступностью данных, повреждением аппаратуры, целостности программного обеспечения;

- идентификация существующих угроз безопасности и уязвимостей, делающих возможным осуществление угроз;

- вычисление рисков, связанных с осуществлением угроз безопасности.

Величина риска определяется на основе стоимости ресурса, вероятности осуществления угрозы нарушения безопасности информационного контура фирмы. Задача управления рисками заключается в выборе обоснованного набора контрмер, позволяющих снизить уровни рисков до приемлемой величины. Стоимость реализации контрмер должна быть меньше величины возможного ущерба. Разница между

стоимостью реализации контрмер и величиной возможного ущерба должна быть обратно пропорциональна вероятности причинения ущерба.

В ходе проведения аудита системы безопасности обычно решаются следующие задачи:

- анализ достаточности ресурсов АС, включая информационные ресурсы, программные и технические средства, а также людские ресурсы, определение их взаимосвязи, расположения и способов взаимодействия;

- анализ групп задач, решаемых системой, и бизнес-процессов, возможности системы обеспечивать безопасность информации при возникновении чрезвычайных ситуаций;

- оценка критичности информационных ресурсов, а также программных и технических средств с учетом вероятности наступления чрезвычайного происшествия;

- определение наиболее вероятных угроз безопасности в отношении ресурсов АС и уязвимостей защиты, делающих возможным осуществление этих угроз;

- оценка вероятности осуществления угроз, величины уязвимостей и ущерба, наносимого организации в случае успешного осуществления угроз;

- определение величины рисков для каждой тройки: угроза - группа ресурсов - уязвимость.

Оценка рисков может даваться с использованием различных, как качественных, так и количественных, шкал. Главное, чтобы существующие риски были правильно идентифицированы и расставлены по приоритетам в соответствии со степенью их критичности для фирмы. На основе такого анализа может быть разработана система первоочередных мероприятий по уменьшению величины рисков до приемлемого уровня.

Второй подход, самый практичный, опирается на использование действующих стандартов информационной безопасности, доступ к которым открыт для всех пользователей. Стандарты определяют базовый набор требований безопасности для широкого класса информационных систем. Сотрудник службы внутреннего контроля в данном случае должен правильно определить набор требований стандарта, соответствие которым необходимо для данной информационной системы.

Из-за своей простоты (набор требований для проведения проверки уже заранее определен стандартом) и надежности (стандарт есть стандарт, и его требования никто не попытается оспорить) описанный подход наиболее распространен на практике, поскольку позволяет при минимальных затратах ресурсов делать обоснованные выводы о состоянии информационной системы фирмы, а значит, спрогнозировать возможности сохранения данных в рамках реализации плана ОНиВД.

Подразделение внутреннего контроля оценивает применимость требований стандарта к АС и ее соответствие этим требованиям. Данные о соответствии различных областей функционирования АС требованиям стандарта обычно представляются в табличной форме. Затем делаются соответствующие выводы и даются рекомендации по реализации в системе механизмов безопасности.

Третий подход, наиболее эффективный, предполагает комбинирование первых двух.

Базовый набор требований безопасности, предъявляемых к информационной системе, определяется международными рекомендациями. Дополнительные требования, в максимальной степени учитывающие особенности функционирования данной информационной системы, формируются на основе анализа рисков. Этот подход намного проще первого, так как большая часть требований безопасности уже определена стандартом, и в то же время он лишен недостатка второго подхода, заключающегося в том, что требования стандарта могут не учитывать специфики обследуемой информационной системы.

Рекомендации по результатам анализа состояния АС определяются используемым подходом, особенностями обследуемой информационной системы, состоянием дел с информационной безопасностью и степенью детализации, используемой при проведении проверки.

Отчет о состоянии информационной безопасности фирмы является основным результатом проведения проверки. Его качество характеризует качество работы по проведению проверки АС. Структура отчета может существенно различаться в зависимости от характера и целей проводимой проверки. Однако определенные разделы должны обязательно в нем присутствовать. Он должен содержать описание целей проведения проверки, характеристику обследуемой АС, указание границ проведения обследования и используемых методов, результаты анализа данных, выводы, обобщающие эти результаты и содержащие оценку уровня защищенности автоматизированной системы или соответствия ее требованиям стандартов, и, конечно, рекомендации по устранению существующих недостатков и совершенствованию системы защиты.

Отчет о состоянии системы информационной безопасности фирмы должен быть в обязательном порядке инкорпорирован в систему ОНиВД фирмы. Это означает, что все перечисленные методы, приемы, подходы, результаты анализа системы информационной безопасности должны иметь понятный вектор, направленный на определение способности АС и ее ресурсов обеспечить непрерывность деятельности фирмы, безопасность ее информационных ресурсов в случае чрезвычайного происшествия [1].

Что же касается непосредственно плана ОНиВД, то в нем отдельным блоком следует выделить такие обязательные мероприятия, как:

- резервное копирование данных и наличие резервных серверов;

- процедуры восстановления функционирования и (или) осуществления информационной поддержки в течение времени использования, разработки, настройки и обслуживания автоматизированных информационных систем;

- осуществление контроля безопасности и обоснованности доступа к системам, программам, оборудованию, данным;

- заключение договоров с провайдерами с целью успешной реализации плана ОНиВД, страхования рисков и компенсации убытков в случае непредвиденных сбоев в информационной системе.

Кроме того, сотрудники подразделения информационных технологий должны быть готовы к работе в нештатной ситуации и мероприятиям по восстановлению и

возобновлению деятельности. В связи с этим благоразумно включить в программу тестирования планов ОНиВД проверку навыков работы ИТ-сотрудников в чрезвычайной ситуации.

Вопрос 3. СОСТАВЛЕНИЕ ВОПРОСНИКА ДЛЯ АУДИТА СИСТЕМЫ БЕЗОПАСНОСТИ ФИРМЫ В РАМКАХ ОНиВД

Очевидно, что оценка уровня обеспечения безопасности фирмы в случае чрезвычайной ситуации довольно субъективна, так как является результатом профессионального суждения сотрудника внутреннего контроля. Снижение фактора субъективизма возможно при проведении тестирования плана ОНиВД и, так сказать, "полевых" испытаний систем безопасности фирмы.

Наиболее применимой методикой для оценки безопасности фирмы в рамках плана ОНиВД могут быть разработка комплексного вопросника аудита систем безопасности и присвоение баллов за тот или иной ответ. Шкала значимости ответов разрабатывается самим руководством фирмы в зависимости от приближения ответа (соответствия фирмы) к международным стандартам обеспечения непрерывности деятельности. Кстати, такая шкала может и не разрабатываться, так как ответ на составленные вопросы и так будет характеризовать качество мероприятий с точки зрения обеспечения информационной и физической защищенности фирмы от внешних воздействий.

Перечень вопросов должен охватывать всю систему мер по обеспечению безопасности фирмы. К примеру:

- определены ли лица/подразделения в плане ОНиВД, ответственные за обеспечение безопасности по конкретным направлениям;

- содержит ли план ОНиВД главные компоненты и мероприятия обеспечения безопасности активов фирмы и персонала;

- определены ли компоненты, механизм и приемлемые методы тестирования и обновления плана ОНиВД;

- проводятся ли фирмой процедуры обработки данных системы локальной сети (LAN) и интернет-сети, компьютерных сетей, каталога адресов электронной почты сотрудников фирмы, программ резервирования данных и их обновления; копирования информации о счетах клиентов, сохранения ее за пределами основного офиса; обновления базы данных; обнаружения нелегально установленных программ;

- разработаны ли подробные инструкции поведения сотрудников фирмы при чрезвычайных происшествиях, насколько проработан план мероприятий обеспечения безопасности активов и персонала в этих инструкциях;

- разработаны, соблюдаются и распространяются ли списки лиц и компаний, которые окажут помощь в ликвидации последствий происшествий для фирмы;

- может ли фирма обеспечить доступ к необходимым ресурсам для обеспечения

безопасности персонала, оборудования, информации;

- имеются ли на фирме устройства сигнализации о тревоге, маршруты эвакуации, список номеров телефонов подразделений, ответственных за ликвидацию последствий чрезвычайного происшествия, устройства отключения коммунальных услуг;

- разработаны, соблюдаются и периодически пересматриваются ли должностные инструкции, полномочия и подчиненность по всему персоналу и для аварийных ситуаций;

- подготовлен ли резервный офис на случай прерывания деятельности основного, предусмотрена ли в нем возможность восстанавливать функции процессинга сервисной компании, включая сохранение библиотек файлов и соответствующих поставок информации для процессинга, микрофильмирования и защиты;

- существуют ли аварийные системы подачи продуктов питания, воды, первой помощи, противопожарных средств;

- разработана, соблюдается и проводится ли учебная программа по проверке плана ОНиВД для сотрудников фирмы на всех уровнях управления фирмой и т.д.

Данный перечень вопросов не является исчерпывающим. Чем детальнее он будет, тем больше вероятность у подразделения службы внутреннего контроля обнаружить возможную проблему, связанную с обеспечением безопасности в случае наступления чрезвычайного происшествия.

В проведении самооценки системы безопасности фирмы главное - это возможность выставления справедливых оценок без последствий для ответственных подразделений в виде лишений премий, выговоров и прочих взысканий. В противном случае фирма рискует получить завышенную оценку системы безопасности, не отражающую истинного положения вещей, а в случае чрезвычайного события он понесет серьезные потери материальных и нематериальных активов.

По итогам аудита оценки плана ОНиВД на предмет обеспечения безопасности для фирмы подразделение внутреннего контроля должно разработать рекомендации и требования для конкретных подразделений фирмы, а затем провести повторный аудит с целью проверки их внедрения.

<1> Юденков Ю.Н., Тысячникова Н.А., Сандалов И.В., Ермаков С.Л. Интернет-технологии в банковском бизнесе: перспективы и риски: Учебно-практическое пособие. М.: КноРус, 2010.

Практическое занятие 3

СИСТЕМНЫЙ ПОДХОД В ОБЕСПЕЧЕНИИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Учебные вопросы:

1. Основные понятия и определения финансовой безопасности.
2. Важность системности при обеспечении финансовой безопасности предприятия.
3. Структура системы обеспечения финансовой безопасности.

Введение

В условиях нестабильности современной мировой экономики и, как следствие, возрастающих угроз для бизнеса наличие адекватной системы управления финансовой безопасностью компании многократно возрастает. Каковы ее основные практические аспекты и каким образом повысить эффективность противодействия финансовым угрозам?

Актуальность разработки стратегии финансовой безопасности (далее - ФБ) компании в период падения спроса и производства связана с целым рядом негативных факторов:

- угрозой уменьшения запаса финансовой прочности компании по отношению к возможным потерям и убыткам, в том числе за счет хищений, халатности и ошибочных действий персонала;

- учащением случаев недобросовестных действий менеджеров и сотрудников;

- повышенным риском мошенничества со стороны контрагентов и др.

Вопрос 1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

В чем же заключаются сущность и особенности понятия финансовой безопасности? Она обычно рассматривается как важнейший элемент общей экономической безопасности фирмы. Анализ точек зрения на понятие ФБ, содержащихся в российском законодательстве и доступной корпоративной практике, позволяет дать следующее авторское трактование: финансовая безопасность представляет собой такое состояние финансовой системы предприятия, при котором возможные угрозы нанесения ущерба его активам, утраты ликвидности, устойчивости и независимости бизнеса, а также прав собственности снижены до приемлемого (нормативного) уровня и поддерживаются на этом либо более низком уровне.

Иными словами, под системой обеспечения ФБ предприятия понимается совокупность

осуществляемого комплекса мер в интересах защиты бизнеса от внутренних и внешних отрицательных финансовых угроз. Степень данной защиты обусловлена способностью органов управления компании на соответствующих уровнях:

- обеспечить устойчивое экономическое развитие фирмы, достижение основных целевых параметров деятельности при сохранении ликвидности и независимости ее финансовой системы;

- нейтрализовать негативное воздействие кризисных явлений экономики, преднамеренные действия конкурентов и иных "недружественных" структур;

- предотвратить сделки с активами предприятия, создающие угрозу утраты прав собственности;

- сформировать адекватную систему учета финансовых потоков и укрепить операционную эффективность системы контроля;

- привлечь и использовать заемные средства по оптимальной стоимости у надежных банков и контролировать приемлемый уровень долговой нагрузки;

- предотвратить случаи халатности, мошенничества, а также преднамеренные действия персонала в отношениях с контрагентами, а также иные финансовые нарушения, в том числе связанные с использованием государственных бюджетных средств;

- разработать и внедрить систему постоянного мониторинга финансового состояния компании с целью раннего диагностирования кризисных явлений и признаков банкротства;

- обеспечить проведение работ по защите конфиденциальности информации, составляющей коммерческую тайну.

Реализация перечисленных направлений поможет предприятию создать необходимый запас прочности финансовой системы перед лицом существующих и вновь возникающих для него угроз.

К сожалению, управление ФБ часто осуществляется в условиях относительно стабильного функционирования бизнеса, когда используется "реактивная" форма управления: принятие управленческих решений для реагирования на текущие проблемы. Безусловно, нельзя сказать, что при этом компании не уделяют внимания вопросам обеспечения защиты своих финансовых интересов и стабильности бизнеса. На многих из них созданы и функционируют службы внутреннего контроля, специальной и экономической безопасности, новомодные подразделения по управлению рисками, внедряются современные информационные системы, системы финансового планирования и прогнозирования. Однако каждая из этих систем нацелена на решение своих локальных задач.

Вопрос 2. ВАЖНОСТЬ СИСТЕМНОСТИ ПРИ ОБЕСПЕЧЕНИИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Между тем наиболее эффективным способом управления ФБ является внедрение системного подхода, включающего в себя введение руководством и собственниками предприятий единых требований ко всем элементам системы управления компанией и организации контроля их исполнения, распределение сфер ответственности по всем категориям персонала вплоть до рядовых сотрудников компании, установление нормативных значений показателей финансовой безопасности.

Особенно важно, чтобы системный подход нашел свое отражение в соответствующем корпоративном документе, например, стратегии экономической безопасности фирмы. В указанном документе должны быть формализованы цели и объекты данной стратегии и ее ключевого элемента - финансовой безопасности. Должны быть определены характеристики угроз ФБ, отражающие специфику ее деятельности, сформулированы критерии и нормативные параметры безопасного финансового состояния бизнеса, описаны меры и механизмы, направленные на его обеспечение. В целях развития основных положений стратегии внутренними локальными нормативными актами предприятия на генерального и финансового директора, руководителей служб безопасности и внутреннего контроля возлагается ответственность за разработку количественных и качественных значений критериев ФБ, мониторинг и прогнозирование факторов, определяющих возникновение финансовых угроз и выработку мер их преодоления, разработку и внедрение систем раннего диагностирования кризисных ситуаций.

Примечание: наиболее эффективным способом управления финансовой безопасностью является системный подход...

Если рассматривать наличие аналогичных документов на макроуровне, то доктрина экономической безопасности нашей страны, в том числе финансовой, утверждена Указом Президента РФ N 608 "О Государственной стратегии экономической безопасности РФ (Основных положениях)". Во исполнение положений данного Указа было принято Постановление Правительства РФ N 1569 "О первоочередных мерах по реализации Государственной стратегии экономической безопасности РФ...".

Основные отличия от системы управления финансами.

Рассматривая вопросы ФБ, нельзя не сказать об отличиях управления финансовой безопасностью от системы управления финансами предприятия.

Так, стратегия финансовой безопасности помимо сценария функционирования компании в так называемых штатных условиях определяет и направления действий руководства в условиях нестабильной (кризисной) ситуации, среди которых можно отметить:

- организацию проведения постоянного мониторинга финансового состояния с целью раннего диагностирования кризисных явлений;

- оценку потенциальных возможностей (внешних и внутренних) по преодолению угрозы финансового кризиса;

- определение перечня мер по предотвращению угроз ФБ;

- оценку эффективности планируемых мер с точки зрения нейтрализации негативных факторов;

- оценку стоимости предлагаемых мер, сроки реализации, ожидаемые результаты финансовой стабилизации.

При этом особенностью управления ФБ является то, что в кризисных условиях принятие управленческих решений часто осуществляется в обстановке снижения общего уровня управляемости компанией.

Однако главное отличие системы управления финансовой безопасностью от процессов финансового управления заключается в том, что основным показателем ее эффективности является соблюдение нормативного уровня параметров и индикаторов финансовой безопасности. Система же управления финансами предполагает проведение оценки финансового состояния предприятия посредством определения размеров отклонений фактических значений показателей от предусмотренных планом либо достигнутых темпов роста. Для выявления угроз ФБ недостаточен анализ изменений указанных индикаторов по годам, за отчетный период или в сравнении с аналогами. Такой анализ не дает четкого ответа, насколько критична ситуация, каков уровень угрозы для бизнеса.

Таким образом, при управлении финансовой безопасностью необходимо сравнение фактических и прогнозных данных с нормативными значениями, четко определяющими параметры кризисной ситуации для данного предприятия, и поддержание показателей не ниже установленного уровня. Перечень пороговых (нормативных) значений ФБ должен быть уже, чем список показателей, применяемых для анализа достижения плановых параметров компании. Он должен быть достаточным для того, чтобы отражать главные направления бизнеса, выявлять наиболее серьезные угрозы финансовой безопасности.

Вопрос 3. Структура системы ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Несколько слов хотелось бы сказать относительно структуры корпоративных органов, обеспечивающих ФБ. В рамках системы ее управления международными стандартами предусматривается необходимость построения и четкого определения иерархии ответственности и полномочий в вопросах безопасности, в том числе прямой ответственности за финансовую безопасность со стороны высшего руководства (руководитель предприятия и финансовый директор). Вместе с тем с организационной точки зрения в эту систему вовлечены практически все сотрудники предприятия, представляющие различные подразделения и уровни управления.

В общем виде система корпоративных органов, обеспечивающих ФБ, включает в себя стратегический и оперативно-тактический уровни, а также соответствующие процедуры и инструментарий обеспечения на каждом из них.

Возглавляет данную систему совет директоров (СД), как правило, орган, представляющий интересы собственника и призванный обеспечить гармонизацию и

повышение эффективности взаимодействия управленческих служб разных уровней. Условно компетенцию СД в обеспечении ФБ можно разделить на две сферы:

а) утверждение стратегии финансовой безопасности;

б) формирование системы обеспечивающих органов.

Постоянно действующим органом финансового контроля, образуемым СД и подотчетным ему, является ревизионная комиссия (дополнительно могут быть созданы комитеты по внутреннему аудиту, экономической безопасности).

Непосредственную реализацию функций по обеспечению ФБ осуществляют подотчетные генеральному директору службы: финансово-экономическая, внутреннего контроля, экономической безопасности и другие.

Безусловно, важнейшим органом, обеспечивающим финансовую безопасность, является финансово-экономический блок, осуществляющий выработку единой финансовой, кредитной, учетной политики.

Основным условием обеспечения ФБ является подготовка и повышение квалификации кадров, разрабатывающих и обеспечивающих реализацию экономической, финансовой, налоговой, денежно-кредитной политики хозяйствующего субъекта. К ним относятся: финансовые директора (менеджеры), главные бухгалтеры, казначеи, внутренние аудиторы, ревизоры и инспекторы. Требования к уровню и качеству профессиональной подготовки данных сотрудников в последнее время существенно возросли не только со стороны самих предприятий как работодателей, но и государства.

Порядок организации и функционирования рассматриваемой системы зависит от масштабов и сложности корпоративной структуры. В частности, небольшие предприятия могут использовать более простые схемы, процессы и процедуры для достижения своих целей в области финансовой безопасности.

Вывод: своевременный акцент на ключевых аспектах ФБ особенно важен в условиях нестабильности внешней и внутренней экономической среды, поскольку только эффективное функционирование системы финансовой безопасности и наличие ее стратегии поможет обеспечить сохранение и дальнейшее успешное развитие бизнеса.

Практическое занятие 4

ОБЕСПЕЧЕНИЕ КАДРОВОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ И ОРГАНИЗАЦИЯХ

Учебные вопросы:

1. Основы обеспечения кадровой безопасности в государственных органах и организациях.
2. Угрозы кадровой безопасности.
3. Основные меры обеспечения кадровой безопасности

Вопрос 1 ОСНОВЫ ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ ОРГАНАХ И ОРГАНИЗАЦИЯХ

Кадровая безопасность является составной частью системы общей безопасности организации наряду с другими составляющими - финансовой, силовой, информационной, технико-технологической, правовой, экологической и др. Главной целью обеспечения безопасности организации являются достижение максимальной стабильности ее функционирования, а также создание основы и перспектив роста для выполнения ее целей вне зависимости от объективных и субъективных угрожающих факторов (негативных воздействий, факторов риска). Сказанное справедливо для организаций любой формы собственности, а также для государственных органов.

Определить кадровую безопасность можно как состояние защищенности организации от угроз, обусловленных человеческим фактором (к ним можно отнести шпионаж, воровство, халатность, ошибки и пр.).

Обеспечение кадровой безопасности - это процесс предотвращения негативных воздействий на организацию за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом [1]. Кадровая безопасность обеспечивается своевременным выявлением, предупреждением и пресечением опасных действий персонала.

Кадровая безопасность занимает ведущее место среди других элементов системы безопасности организации, т.к. она связана с персоналом, кадрами, которые, как известно, "решают все". М.В. Жижина указывает на то, что персонал является одним из основных факторов риска экономической безопасности предприятия. Указанный автор приводит следующие доводы: более трех четвертей правонарушений (в т.ч. преступлений) в организациях совершаются сотрудниками, при этом большая часть правонарушений обнаруживается случайно [2].

Коммерческие организации довольно давно обратили внимание на проблему обеспечения кадровой безопасности. Она напрямую связана с вопросом обеспечения сохранности коммерческой и служебной тайн организации. Государственные же органы и организации зачастую пренебрегают данным вопросом. Представляется, что

теоретические и практические разработки, сделанные для бизнеса, могут быть использованы в работе государственных органов и организаций.

Вопросы кадровой безопасности в государственных органах и организациях нечасто, но все же становятся объектом исследования в юридической литературе. Следует отметить работы И.О. Башмачниковой, А.В. Горожанина, Г.Е. Журавлевой, Г.М. Мякишева, А.Д. Сафронова и др., посвященные кадровому потенциалу и кадровой безопасности органов внутренних дел [3, 4, 5, 6, 7]. Имеются некоторые работы, в т.ч. методологического характера об отборе и подготовке кадров на государственную службу и общественную работу [8]. Внимание уделено даже историческому аспекту данной проблемы [9]. Но все же следует отметить, что проблема кадровой безопасности государственных учреждений не стала объектом пристального внимания не только теоретиков, но и практиков - руководителей государственных структур и организаций.

Вопрос 2. УГРОЗЫ КАДРОВОЙ БЕЗОПАСНОСТИ

Для обеспечения кадровой безопасности следует различать внешние и внутренние угрозы.

Внешние негативные воздействия - это действия, явления или процессы, не зависящие от работников организации и влекущие нанесение ущерба (например, попадание сотрудников в различные виды зависимости, инфляционные процессы).

В свою очередь, к внутренним негативным воздействиям относятся действия сотрудников организации, влекущие нанесение ущерба (например, несоответствие квалификации сотрудников предъявляемым к ним требованиям или недостаточная квалификация сотрудников; слабая организация системы управления персоналом; слабая организация системы обучения; неэффективная система мотивации; ошибки в планировании ресурсов персонала; снижение количества рационализаторских предложений и инициатив; уход квалифицированных сотрудников; ориентация сотрудников на решение внутренних тактических задач; ориентация сотрудников на соблюдение интересов подразделения; некачественные проверки кандидатов при приеме на работу и др.).

Указанные негативные процессы характерны не только для коммерческих организаций, но и для государственных. Представляется логичным сделать вывод о том, что работа коммерческих организаций по обеспечению кадровой безопасности, включающая в себя как минимум три составляющие: наем, лояльность и контроль, должна быть организована и в государственных органах.

Вопрос 3. ОСНОВНЫЕ МЕРЫ ОБЕСПЕЧЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТИ

Для обеспечения кадровой безопасности государственным органам и организациям следует проводить более тщательные проверки кандидатов на должности, т.к. это

делается в правоохранительных органах. Если соискатель, например, имеет связи с криминальными структурами, он способен нанести вред интересам организации. Если его родственники трудятся в коммерческих фирмах, вполне вероятны утечка важной информации, использование служебного положения в целях "помощи" родственникам. Если потребность в расходах кандидата на должность, предполагающую материальную ответственность, высока, а общий доход семьи незначителен, он тоже попадает в группу риска. Необходимо также внимательно изучить деловую репутацию претендента.

Практика проверки кандидата на должность и членов его семьи в настоящее время реализуется в правоохранительных органах (Приказ МВД России от 19.05.2009 N 386 "О порядке отбора граждан на службу (работу) в органы внутренних дел Российской Федерации" (вместе с Инструкцией о порядке отбора граждан на службу (работу) в органы внутренних дел Российской Федерации). Например, при поступлении на службу (работу) в федеральную противопожарную службу проводится проверка сведений, представленных кандидатами на службу (работу) с целью выявления их достоверности, а также выявления сведений, являющихся ограничениями в приеме на службу (работу) в федеральную противопожарную службу МЧС России (Приказ МЧС России от 11.11.2009 N 626 "О порядке отбора граждан на службу (работу) в федеральную противопожарную службу" (вместе с Инструкцией о порядке отбора граждан на службу (работу) в федеральную противопожарную службу).

Проверка проводится с письменного согласия проверяемого лица путем использования возможностей органов внутренних дел Российской Федерации. Проверка подразделяется на полную, неполную, местную и дополнительную. Первые два вида проверок проводятся в отношении кандидата, его жены (мужа) и их детей. Местная проверка проводится в отношении самого кандидата по учетам органов внутренних дел.

При приеме на службу в органы наркоконтроля (ФСКН России) проводится среди прочего предварительное изучение кандидата на должность в форме собеседования, ознакомления с документами гражданина (Приказ ФСКН России от 08.10.2009 N 444 "Об утверждении Инструкции о порядке приема на службу, испытания при приеме на службу, назначения на должности, заключения контрактов о прохождении службы, освобождения от должностей и присвоения специальных званий в органах по контролю за оборотом наркотических средств и психотропных веществ").

В процессе этих мероприятий выясняются мотивы поступления на службу в органы наркоконтроля и в конкретное структурное подразделение органа наркоконтроля, соответствие имеющегося профессионального образования квалификационным требованиям по уровню образования по предполагаемой должности, наличие опыта работы по специальности, сведения о привлечении его к административной, уголовной ответственности и другие сведения, необходимые для принятия решения о проведении проверки гражданина для приема на службу в органы наркоконтроля.

В процессе предварительного изучения гражданина с его согласия осуществляется посещение его по месту жительства, проводится беседа с его родителями, женой (мужем).

Очевидно, что подобного рода проверки нецелесообразны, а порой и невозможны во всех государственных структурах, однако представляется необходимым уделять

кандидатам на должности в государственных органах и организациях более пристальное внимание.

Проблема лояльности

В современных условиях для российских организаций все большее значение приобретают вопросы мотивации организационного поведения, особенно лояльности к организации. Лояльность персонала предполагает собой преданность руководителю, фирме и делу [10].

Лояльность - довольно сложное понятие, которое означает преданность, верность. Это эмоционально окрашенное отношение к компании, желание быть полезным, нужным, делать как можно больше хорошего, предупреждать об опасности. Лояльный сотрудник всегда стремится быть честным и искренним по отношению к компании, выполнить свою работу наилучшим образом и готов даже приносить определенные жертвы во имя успехов организации, испытывая чувство гордости за ее победы, имеет сильное желание оставаться членом данной организации, несмотря на возникающие проблемы и сложности в ее работе, полон энтузиазма и желания помогать в решении этих проблем [10].

Организационная лояльность - это связи сотрудника и организации, базирующиеся на ценностных нормах, принимаемых сотрудником и соответствующих требованиям организации.

Работа вызывает у лояльных сотрудников удовлетворенность содержанием работы, выполняемой в организации, ощущение внимания и заботы со стороны организации, удовлетворенность своей карьерой в организации, уверенность в целесообразности длительной работы в данной организации.

Соответственно, сотрудники государственных органов и организаций, заработная плата которых относительно низкая, в то же время ответственность и уровень контроля высок, вряд ли удовлетворены своей работой в данной организации.

Контроль представляет собой комплекс мер, установленных для персонала и содержащихся, например, в регламентах, объединяющих ограничения, режимы, технологические процессы, оценочные, контрольные и другие операции. Это комплекс непосредственно нацелен на ликвидацию возможностей причинения ущерба. Как правило, главная роль в осуществлении контроля принадлежит службе безопасности или другим подразделениям и в меньшей степени службе персонала.

Комплекс мер

Кадровая безопасность государственной организации (и государственного органа) должна достигаться путем решения следующих задач:

1. Выявление и пресечение угроз, исходящих от персонала: криминальная деятельность, разглашение тайн, сотрудничество с бизнес-структурами, негативные психолого-физиологические и морально-нравственные проявления.

2. Сбор сведений о кандидатах на работу для принятия руководством решений о приеме или отказе.

3. Сбор и анализ сведений о сотрудниках для принятия решений о допуске к

конфиденциальным документам или участию в важных проектах.

4. Социально-психологическое обеспечение управления персоналом, изучение обстановки в трудовых коллективах и взаимоотношений между сотрудниками.

5. Обучение и подготовка персонала по вопросам соблюдения мер безопасности и правил обращения с конфиденциальной информацией.

6. Проведение служебных расследований по фактам поведения сотрудников, наносящих ущерб безопасности организации.

Актуальным для государственных органов являются и разумный подбор и расстановка сотрудников с использованием современных средств подбора персонала; продуманная и документированная система служебного роста и денежного вознаграждения сотрудников; создание в коллективе благоприятного климата взаимоотношений для работы персонала и объективное рассмотрение данных вопросов с доведением результатов до всех сотрудников с целью исключения конфликтных ситуаций, которые могут привести к негативным последствиям.

Вся эта деятельность не является отдельным направлением в функционале отдела кадров, а лишь органично вписывается в него. И здесь практически не привлекаются какие-либо дополнительные ресурсы при условии, что в организации присутствуют все этапы организации и управления персоналом.

Государственным органам и организациям следует ввести в функционал сотрудников кадрового подразделения информационно-аналитическую составляющую, когда происходят анализ и оценка выявленных внутренних рисков, прогноз развития событий, планируют меры по обеспечению организационно-кадровой безопасности и координируют работу по их реализации.

Многие государственные органы (МВД, ФСБ, таможня и др.) имеют кадрово-психологическую службу, которая осуществляет отбор и проверку персонала предприятия при приеме на работу и в процессе труда, выявляет и локализует риски, обусловленные человеческим фактором.

Таким образом, кадровая безопасность нацелена на такую работу с персоналом, на установление таких трудовых и этических отношений, которые будут способствовать развитию и успешному функционированию данной организации. Кадровой безопасности в государственных органах и организациях следует уделять повышенное внимание.

Библиография

1. Чумарин И.Г. Что такое кадровая безопасность компании? // Кадры предприятия. 2003. N 2.

2. Жижина М.В. Обеспечение кадровой безопасности предприятия и почерковедения // Безопасность бизнеса. 2008. N 1. С. 43.

3. Башмачникова И.О. Кадровый потенциал правоохранительных органов в условиях

нового типа экономических отношений: типология категории и ее понимание // Вестник Академии экономической безопасности МВД России. 2009. N 10. С. 85 - 89.

4. Горожанин А.В. Кадры органов внутренних дел: Современные проблемы обеспечения / Под ред. В.П. Сальникова. СПб.: Фонд поддержки науки и образования в области правоохранительной деятельности "Университет", 1999. 160 с.

5. Журавлева Г.Е. К проблеме отбора на службу в органы внутренних дел Российской Федерации по конкурсу // Вестник Академии экономической безопасности МВД России. 2009. N 2. С. 121 - 124.

6. Мякишев Г.М. О кадровом потенциале органов внутренних дел и его прогнозировании // Вестник Академии экономической безопасности МВД России. 2008. N 2. С. 122 - 123.

7. Сафронов А.Д. Запрещающие нормы в российском праве и проблемы кадровой безопасности в органах внутренних дел // Труды Академии управления МВД России. 2009. N 4. С. 58 - 65.

8. Радионов Г.А., Иванов М.Н., Задерей В.А. Стратегия формирования системы подготовки кадрового резерва для общественной работы и государственной службы // Национальная безопасность и геополитика России. 2001. N 11 - 12 (28 - 29). С. 129 - 132.

9. Байкеева С.Е. Научно-правовые идеи ученых дореволюционной России о государственной службе и ее кадровом обеспечении // Юристъ-Правоведъ. 2008. N 4. С. 81 - 85.

10. Ветошкина Т. Кадровая безопасность и лояльность персонала // Кадровик. Кадровый менеджмент. 2009. N 1. С.12.

Практическое занятие 5

ПРАВОВЫЕ АСПЕКТЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ В УСЛОВИЯХ КОРПОРАТИВНЫХ КОНФЛИКТОВ

Учебные вопросы:

1. Правовая основа информационной безопасности.
2. Система правового регулирования информационной безопасности.

Вопрос 1. ПРАВОВАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Проблема обеспечения общественной безопасности в современных условиях приобрела особое значение среди многих других социальных проблем. Для ее решения требуются соответствующие силы, средства и ресурсы, специальные структуры, управленческие кадры и специалисты-профессионалы, научное, организационное, правовое и иное обеспечение, единая выверенная и взвешенная политика национальной безопасности, охватывающая все основные сферы жизни и деятельности общества и государства и, самое главное, в условиях демократического правового государства - надежная и эффективная правовая база <1>. Актуальность проблемы связана с тем, что общественная безопасность - один из основных факторов существования и прогрессивного развития личности, общества и государства, международной безопасности. Важнейшей составной частью системы общественной безопасности является экономическая безопасность государства.

<1> Есаян А.К. Криминологические основы обеспечения евразийской экономической безопасности: Автореф. дис. ... докт. юрид. наук. М., 2011. С. 4.

В Государственной стратегии экономической безопасности России к числу "наиболее вероятных угроз экономической безопасности" отнесена криминализация общества и хозяйственной деятельности <2>. Она представляет собой наиболее серьезную проблему. В первую очередь это обусловлено факторами, к числу которых относятся рост безработицы, поскольку значительная часть преступлений совершается теми, кто не имеет постоянного источника дохода; сращивание части чиновников государственных органов с организованной преступностью; доступ криминальных структур к управлению определенной частью производства и их проникновение в различные властные структуры; ослабление системы государственного регулирования и контроля, что привело к расширению деятельности криминальных структур на внутреннем финансовом рынке, в сфере приватизации, экспортно-импортных операций и торговли.

<2> Указ Президента РФ от 29 апреля 1996 г. N 608 "О Государственной стратегии экономической безопасности Российской Федерации (Основных положениях)" // СЗ

РФ. 1996. N 18. Ст. 2117.

В Стратегии национальной безопасности Российской Федерации главными угрозами национальной безопасности в экономической сфере на долгосрочную перспективу названы непрекращающийся рост преступных посягательств, направленных против собственности, наличие условий для усиления криминализации хозяйственно-финансовых отношений <3>.

<3> Указ Президента РФ от 12 мая 2009 г. N 537 "О стратегии национальной безопасности Российской Федерации до 2020 года" // СЗ РФ. 2009. N 20. Ст. 2444.

Усиливающаяся криминализация хозяйственно-финансовых отношений, рост числа новых видов преступлений, в том числе в сфере корпоративных отношений (корпоративных преступлений), связаны с недостатками в правовом регулировании процессов управления, использования финансовых и других материальных ресурсов, отсутствием действенного государственного контроля над экономической деятельностью.

Экономическая преступность за годы реформ приобрела настолько злокачественный характер, что угрожает национальной безопасности государства. Масштабная криминализация коснулась практически всех сфер экономики.

Криминализация экономики как угроза экономической безопасности отмечается многими специалистами <4>. В период проведения реформ страну захлестнули крупномасштабные мошеннические операции в кредитно-финансовой системе: массовый обман населения создателями разного рода финансовых "пирамид" и фондов, нецелевое использование кредитов, присвоение средств, полученных по договорам, криминальные неплатежи.

<4> Пинкевич Т.В. Криминологические и уголовно-правовые основы борьбы с экономической преступностью: Автореф. дис. ... докт. юрид. наук. М., 2002. С. 3, 4; Горелов А.П. Уголовно-правовая охрана сферы предпринимательской деятельности как направление обеспечения экономической безопасности России: Автореф. дис. ... докт. юрид. наук. М., 2004. С. 3, 4; Лунеев В.В. Преступность и теневая экономика // Экономическая наука современной России. 2005. N 1(28); Кутылкин В.А. Экономическая безопасность и противодействие теневым процессам в банковской системе России: Автореф. дис. ... канд. экон. наук. М., 2006. С. 4; Бобков А.В. Криминальное банкротство: криминологическая характеристика и противодействие: Дис. ... канд. юрид. наук. Омск, 2006. С. 3; Кашепов В.П. Корпоративный шантаж: квалификация, ответственность // Российская юстиция. 2006. N 10. С. 14; Клейменов М.П. Криминология: Учебник. М., 2008. С. 420; Пронников А.В. Уголовно-правовая политика в сфере противодействия экономической преступности: Автореф. дис. ... канд. юрид. наук. Омск, 2008. С. 4; Селевич О.С. Банкротство как механизм передела собственности: Автореф. дис. ... канд. экон. наук. Томск, 2010. С. 3; Есаян А.К. Указ. соч. С. 4.

Данные официальной статистики прямо указывают на наличие исключительно опасных угроз экономической безопасности, которые проявляются в форме преступных посягательств. Так, ущерб, причиненный России экономическими преступлениями, в 2009 г. вырос более чем в восемь раз. Выявлено 172,8 тыс. тяжких и особо тяжких преступлений экономической направленности, что составляет 40,3% общего числа преступлений, выявленных в сфере экономики <5>. В 2010 г. ущерб от экономических преступлений достиг 176,42 млрд руб., было выявлено 276,4 тыс. преступлений данной категории, из которых 47,9% - тяжкие и особо тяжкие <6>. Следует учесть и высокую латентность экономической преступности (до 85%) <7>, в силу которой данные официальной статистики в десятки раз меньше реальных показателей.

<5> Состояние преступности в России за 2009 год. М.: ГИАЦ МВД России, 2010. С. 82.

<6> Состояние преступности - январь - декабрь 2010 г. // http://sartraccc.ru/i.php?oper=read_file&filename=Crimstat/short_2010.htm.

<7> Лунеев В.В. Тенденции современной преступности и борьбы с ней в России // Государство и право. 2004. N 1; Он же. Преступность и теневая экономика.

При всем многообразии форм и видов преступлений экономической направленности особую опасность представляют деяния, совершаемые в таких сферах обеспечения экономической безопасности, как финансово-кредитная, внешнеэкономическая, потребительский рынок, сделки с недвижимостью, а также налогообложение.

Для государства сложившаяся ситуация стала одним из главных факторов неблагоприятного инвестиционного климата, препятствующего притоку инвестиций в экономику.

Согласно исследованиям мировых информационных агентств в рейтинге инвестиционной привлекательности Россия стабильно занимает непомерно низкие позиции, где-то по соседству с африканскими странами <8>. И хотя многие высшие должностные лица государства утверждают, что эти данные не отражают действительности, факт остается фактом - иностранные компании не спешат делать долгосрочные инвестиции в российскую экономику.

<8> Таймазов В. Пираты нового времени // Расчет. 2008. N9.

Проведенный специалистами агентства "Bloomberg" и редакции журнала "Слияния и поглощения" в 2010 г. опрос показал, что лишь 10% респондентов (зарубежные инвесторы - представители 1 тыс. иностранных компаний) оценивают российский рынок как наиболее перспективный для инвестиций, остальные (90%) полагают, что инвестиционный климат в России оставляет желать лучшего <9>.

<9> Слияния и поглощения. 2010. N 12. С. 7.

Представители российского бизнеса также скептически относятся к инвестиционному климату в нашей стране. Отечественное предпринимательское сообщество сейчас активно выводит резервные капиталы из российской экономики за рубеж, чтобы прожить там до улучшения ситуации. Согласно сведениям, полученным в результате проведения научных исследований современных тенденций инвестиционной активности внутри российской экономики, на каждый миллиард долларов, вложенный в отечественную экономику зарубежными инвесторами, приходится 3 - 4 млрд долл., выведенных из экономики России <10>. По данным Федеральной службы госстатистики, в 2010 г. отток капитала из России составил около 80 млрд долл. <11>. В связи с этим в 2010 г. Президент РФ Д. А. Медведев и вице-премьер И. Шувалов вынуждены были провести целую серию консультаций и встреч с руководителями американских венчурных фондов и другими зарубежными инвесторами по вопросам того, какие шаги предпринимают власти для снижения инвестиционных рисков, в том числе в направлении нейтрализации угрозы рейдерского захвата, корпоративного шантажа и коррупции <12>.

<10> Дойников И.В. Проблемы предпринимательского (хозяйственного) права // Приложение к журналу "Предпринимательское право". 2010. N 2. С. 3.

<11> Слияния и поглощения. 2010. N 12. С. 6.

<12> Иностранцы ждут погоды // Российская газета. 2010. 17 июня.

Правда, эти меры не дали ожидаемого результата. 30 марта 2011 г. на заседании Комиссии по модернизации и технологическому развитию экономики России Д.А. Медведев констатировал полное отсутствие доверия и заинтересованности отечественных и иностранных инвесторов, назвал инвестиционный климат в стране очень плохим, отметив, что условия для ведения бизнеса для многих компаний в 2011 г. ухудшились, а в возможность безопасной и успешной предпринимательской деятельности верит не так много людей, как хотелось бы руководству государства, в результате деньги бегут из российской экономики.

Путем воздействия на развитие финансовых рынков защита инвесторов оказывает существенное влияние на развитие реального сектора экономики. Развитие финансовых рынков способствует ускорению экономического роста за счет роста сбережений, направления их в реальные инвестиции, поощрения накопления капитала, повышения эффективности распределения ресурсов.

Высокий уровень защиты инвесторов также способствует повышению рыночной стоимости корпораций. Чем надежнее защищены права инвесторов, тем более активно они готовы вкладывать свои деньги в российский бизнес.

К настоящему времени в результате переориентации части экономики на обеспечение интересов криминальных структур и вывоз капитала государство утрачивает инвестиционные ресурсы для развития экономики. Стабилизация экономики, устойчивость валютного курса, рост финансового рынка, обеспечение населения продовольствием оказываются в зависимости от привлечения кредитных ресурсов международных финансовых организаций и иностранных государств. Это явление,

бесспорно, угрожает национальной и экономической безопасности России. В таких условиях функционирующие в Российской Федерации хозяйствующие субъекты сталкиваются со значительными препятствиями в реализации намеченных планов по модернизации производства, развитию бизнеса, привлечению инвестиций, выполнению социальных, налоговых и других обязательств перед трудовым коллективом компании, обществом и государством.

Деятельность корпораций в современных условиях хозяйствования в России остается весьма сложной. Это связано не только с общим кризисным состоянием российской экономики, сохраняющейся инфляцией, низким курсом рубля и прочими макроэкономическими деформациями, но и с рядом специфических факторов, усиливающих активизацию угроз экономической безопасности предпринимательства. Среди таких факторов наибольшее значение имеют следующие:

- значительная степень монополизации рынка, частично сохранившаяся от прежней административно-командной системы, частично возникшая вновь. Одновременно нарастает уровень конкурентной борьбы за российские рынки как со стороны отечественных, так и зарубежных производителей;

- установление контроля криминальных структур над рядом секторов экономики и субъектами хозяйственной деятельности;

- сохранение значительного давления на хозяйствующие субъекты со стороны государственных органов (например, в сферах лицензирования, налогообложения);

- высокий уровень коррупции в органах государственной власти и местного самоуправления;

- рост криминализации российского бизнеса вообще и участившееся использование криминальными структурами сделок в целях отмывания "грязных" денег, вывоза их за рубеж и пр.;

- распространение на всей территории России рейдерских захватов, криминальных банкротств и случаев корпоративного шантажа;

- наличие ряда социальных проблем - низкий уровень доходов населения, безработица, текучесть кадров. Все это снижает степень ответственности и увеличивает вероятность склонности работника к продаже конфиденциальной информации компании и прочим незаконным действиям;

- несовершенство законодательства, регулирующего отношения в сфере предпринимательства (выражающееся, например, в ориентации правовых норм на борьбу с последствиями правонарушений, а не с их причинами, в несоответствии причиненного ущерба и применяемых санкций);

- отсутствие единства действий и взаимной согласованности различных правоохранительных органов;

- относительная "молодость" российского бизнеса и неотработанность средств и методов защиты собственной экономической безопасности, отсутствие опытных специалистов.

Абсолютное большинство отечественных компаний систематически сталкиваются с

угрозами их экономической безопасности. Данная проблема приобретает особую значимость в современных условиях хозяйствования в России. По расчетам некоторых ученых, реальная распространенность преступных посягательств на экономическую безопасность негосударственных хозяйствующих субъектов превышает расчетный регистрируемый показатель в 60 - 65 раз <13>.

<13> Шаваев А.Г. Криминологическая безопасность негосударственных объектов экономики. М., 1995. С. 39; Он же. Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы. М.: Банковский Деловой Центр, 1998. С. 42.

Обеспечение экономических свобод в России также пока находится на неприемлемо низком уровне. По данным исследования "Heritage Foundation" и "The Wall Street Journal", в рейтинге по экономическим свободам по итогам 2010 г. Россия заняла 143 место среди 179 государств. Эксперты обнаружили, что уровень экономической свободы в мире в целом увеличился, а после кризиса возобновился импульс развития. В России вроде бы тоже наблюдалась позитивная динамика, но наша страна не сумела подняться в рейтинге ни на одну позицию. Более того, по данным Комитета по гражданскому законодательству Госдумы, в 2010 г. число индивидуальных предпринимателей в России сократилось с 4,61 до 4,11 млн человек <14>. Данные цифры свидетельствуют о снижении предпринимательской активности населения, вызванной в том числе низким уровнем обеспечения экономических прав и свобод, что абсолютно не согласуется с декларируемой высшими должностными лицами государства политикой по созданию благоприятных условий для развития бизнеса в России.

<14> Рейдерство и коррупция угрожают существованию предпринимателя в России, но бизнес готов к борьбе // http://www.finam.ru/analysis/forecasts0119F/.

Кроме того, предпринимательская деятельность по своей сути является весьма разносторонней. Она связана с решением организационных вопросов, правовыми и экономическими проблемами, техническими и кадровыми аспектами и т.д. Особенно усложняется управление такой деятельностью, когда фирма является крупным диверсифицированным производственным предприятием, которое имеет широчайшие деловые связи и значительное количество контрагентов: поставщиков, кредиторов, заемщиков, клиентов.

В любом случае каждая фирма представляет собой систему, включающую в себя основные элементы и связи между ними. Система - это совокупность объектов, взаимодействие которых обусловливает наличие интегративных качеств, не свойственных ее частям, компонентам <15>. Как раз по линиям внутренних и внешних связей системы (фирмы) и могут реализоваться угрозы ее экономической безопасности. Для обеспечения максимальной степени защиты от этих угроз и необходима определенная деятельность, которая также должна носить системный характер.

<15> Афанасьев В.Г. Системность и общество. М.: Политиздат, 1980. С. 24.

Объектом системы обеспечения экономической безопасности выступает стабильное экономическое состояние хозяйствующего субъекта в текущем и перспективном периоде. Именно от объекта защиты во многом зависят основные характеристики системы обеспечения экономической безопасности. Поскольку объект защиты является сложным, многоаспектным, то эффективное обеспечение экономической безопасности должно основываться на комплексном подходе к управлению этим процессом. Такой подход предполагает учет в управлении объектом всех основных его аспектов и все элементы управляемой системы рассматриваются только в совокупности, целостности, единстве. Реализация данного подхода объективно требует создания комплексной системы обеспечения экономической безопасности предпринимательской деятельности.

Комплексная система обеспечения экономической безопасности предпринимательства - это совокупность взаимосвязанных мероприятий организационно-правового, социально-экономического, технико-технологического, административного, воспитательного, финансового и иного характера, осуществляемых в целях защиты предпринимательской деятельности от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным экономическим потерям. Исследованию отдельных аспектов такой системы посвящены работы представителей экономической, юридической и других наук.

Проблемы применения уголовно-правовых средств охраны отношений в сфере экономики в целом и в сфере предпринимательства в частности освещены в монографических, в том числе диссертационных, и иных исследованиях В.М. Алиева, Д.И. Аминова, А.А. Аслаханова, А.Б. Баранова, А.Г. Безверхова, А.И. Бойцова, Г.Н. Борзенкова, В.А. Ванцева, Б.В. Волженкина, Л.Д. Гаухмана, А.П. Горелова, Ю.Н. Демидова, А.И. Долговой, А.Э. Жалинского, О.Г. Карповича, И.А. Клепицкого, М.П. Клейменова, С.П. Коровинских, С.М. Кочои, Н.Ф. Кузнецовой, А.П. Кузнецова, В.Д. Ларичева, Н.А. Лопашенко, А.И. Лукашова, С.В. Максимова, И.Ю. Михалева, А.В. Наумова, П.Н. Панченко, Т.В. Пинкевич, В.И. Плоховой, Т.Ю. Погосян, П.А. Скобликова, М.В. Талан, В.И. Тюнина, С.В. Устиновой, Т.Д. Устиновой, И.В. Шишко, Е.В. Эминова, П.С. Яни, Б.В. Яцеленко и других ученых.

Вопросы обеспечения роста конкурентоспособности национальной экономики и государственного регулирования экономического развития в условиях трансформации нашли подробное отражение в работах А.А. Аузана, Л.И. Абалкина, В.В. Волкова, Я.И. Кузьминова, В.И. Кушлина, Ю.В. Куроедова, Д.С. Львова, А.М. Марголина, М.И. Одинцовой, В.В. Перской, В.В. Радаева, А.Н. Фоломьева, А.Е. Шаститко, Ю.В. Шишкова, Ю.В. Яковца, Е.Г. Ясина.

Отдельные положения темы исследования, в частности проблемы виктимологической профилактики в системе предупредительного воздействия на преступность и преступления, затрагивались в научных трудах таких выдающихся криминологов, как Ю.М. Антонян, Ю.В. Бышевский, Д.В. Ривман, В.С. Устинов, Л.В. Франк, а также В.В. Вандышев, В.С. Минская, В.И. Полубинский, А.Л. Репецкая, В.Я. Рыбальская, Б.В. Сидоров, Г.И. Чечель, С.Г. Войтенко, А.Н. Красиков, Н.Ф. Кузнецова, В.Е. Квашис, В.П. Коновалов, Э.Ф. Побегайло, О.В. Старков, Е.Е. Центров, Д.А. Шестаков. Некоторым аспектам виктимологической профилактики посвящены работы А.Ю. Арефьева, А.А.

Глуховой, И.В. Ильина, Н.В. Исаева, А.Л. Ситковского и других исследователей.

Актуальные вопросы обеспечения безопасности предпринимателей рассматривались Я.В. Бузановой, Р.Б. Гладких, С.В. Лекаревым, В.Д. Ларичевым, И.В. Гусевым, А.И. Гуровым, Е.С. Жигаревым, М.Н. Зацепиным, А.В. Крысиным, М.В. Лелетовой, С.К. Лесным, В.П. Мак-Маком, А.А. Одинцовым, А.П. Судоплатовым, А.Г. Шаваевым, В.В. Шлыковым, В.И. Яковлевым, В.И. Ярочкиным. Однако до настоящего времени система комплексной защиты предпринимателей от преступных посягательств (предупреждение криминальной виктимизации) остается недостаточно изученной. Исследования же виктимологических аспектов обеспечения экономической безопасности хозяйствующих субъектов в условиях корпоративных конфликтов на монографическом уровне не проводились.

С учетом сказанного полагаем, что чрезвычайную актуальность имеет проведение специального научного исследования, предметом рассмотрения которого должен стать анализ такого элемента обозначенной комплексной системы, как виктимологические аспекты обеспечения экономической безопасности хозяйствующих субъектов в условиях корпоративных конфликтов.

Создание превентивной системы корпоративной безопасности бизнеса является в настоящее время обязательным условием нормальной деятельности любого предприятия, следовательно, и эффективного экономического развития современного российского государства.

Комплексная правовая поддержка бизнеса - обязательный элемент его функционирования. Без этого компания не сможет достойно ответить на вызовы современности, а также обеспечить собственный экономический рост. Все это предопределяет необходимость всесторонне исследовать источники и факторы экономической безопасности предприятия, что позволит разработать рекомендации по дальнейшему развитию законодательной базы предпринимательского оборота и обеспечить безопасность при покупке и продаже бизнеса. Это доказывает актуальность данного направления исследования в теоретическом и практическом аспектах.

Практическое занятие 6

ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СДЕЛОК

Учебные вопросы:

1. Подготовительный этап.
2. Основной этап.
3. Заключительный этап

Введение

Обеспечение безопасности сделки возможно на нескольких уровнях: правовом (юридическом), технологическом и финансовом. Понять, чем они различаются, можно на примере договора купли-продажи квартиры. Правовая проверка (проверка юридической чистоты квартиры) предполагает проверку всех, кто по закону может обладать правом пользоваться данной недвижимостью. Технологическая проверка имеет задачу установить, что квартира свободна от обременения, не находится под арестом. Это особенно важно для квартир, покупаемых через ипотеку. Финансовая проверка подразумевает проверку денежных расчетов по договору (например, проверка банкнот в случае расчетов наличными). Первичным уровнем является юридический, ведь именно от того, насколько с правовой стороны та или иная сделка составлена правомерно и соответствует действующему законодательству, зависит успех предпринимательской деятельности в целом.

Действиями по обеспечению безопасности сделок должны сопровождаться все этапы процесса заключения договора. Таких этапов три: подготовительный (подготовка к подписанию), основной (процесс определения условий договора), заключительный (оформление и непосредственное подписание). Каждый этап имеет свою специфику в обеспечении безопасности сделки.

Вопрос 1. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП

На подготовительном этапе основной задачей является определение отношения организации или индивидуального предпринимателя к предполагаемому договору, а точнее - к потенциальному партнеру.

Здесь следует иметь в виду, что в соответствии с гражданским законодательством граждане и юридические лица свободны в заключении договора (пункт 1 ст. 421 ГК РФ). Это означает, что предпринимателя никто не может принудить к заключению договора, он сам волен выбирать партнера при заключении договора, вид и условия договора.

В то же время необходимо учитывать и существующую в мировой практике доктрину экономической целесообразности сделки, а также осмотрительности и осторожности

участников экономических и гражданских отношений. В нашей стране о необходимости соблюдения такой доктрины свидетельствует позиция КС РФ и арбитражных судов.

Осмотрительность и осторожность. В Постановлении КС РФ от 21.04.2003 N 6-П впервые упоминаются такие качества участника экономических правоотношений, как добрая воля, разумная осмотрительность и осторожность.

По мнению КС РФ, конституционные принципы свободы экономической деятельности и свободного перемещения товаров, услуг и финансовых средств предполагают наличие надлежащих гарантий стабильности, предсказуемости и надежности гражданского оборота, которые не противоречили бы индивидуальным, коллективным и публичным правам и законным интересам его участников. Поэтому, осуществляя в соответствии со ст. 71 (п. п. "в" и "о") и ст. 76 Конституции РФ регулирование оснований возникновения и прекращения права собственности и других вещных прав, договорных и иных обязательств, оснований и последствий недействительности сделок, федеральный законодатель должен предусматривать такие способы и механизмы реализации имущественных прав, которые обеспечивали бы защиту не только собственникам, но и добросовестным приобретателям как участникам гражданского оборота.

Исходя из положений изложенных норм, должная осмотрительность и осторожность налогоплательщика как участника экономических отношений гарантирует осуществление в отношении него правовой защиты. Таким образом, данные положения еще раз подчеркивают принцип презумпции добросовестности налогоплательщика.

Эти положения развивает и судебная практика. Так, арбитражные суды приходят к выводу, что, учитывая основополагающие принципы гражданского законодательства, участники гражданского оборота при совершении каких-либо действий в рамках прав, предоставленных законодательством, должны действовать с должной мерой осмотрительности и осторожности, без причинения вреда другому лицу либо себе <1>.

Суды отмечают, что налогоплательщики обязаны изучить первичные документы, подтверждающие право собственности контрагента на предмет договора купли-продажи, а в случае если не делают этого, то они не проявляют должной осмотрительности и осторожности <2>.

Федеральный арбитражный суд Западно-Сибирского округа в Постановлении от 26.06.2006 N Ф04-3624/2006(23675-А46-25) отмечает, что в силу ст. 2 Гражданского кодекса РФ (далее - ГК РФ) предпринимательская деятельность осуществляется предприятиями на свой риск, в связи с чем на них возлагается бремя несения возможных неблагоприятных последствий, а также определенной ответственности в ходе ее осуществления. Это, в свою очередь, означает, что каждое юридическое лицо обязано соблюдать определенного рода осторожность и осмотрительность в делах, особенно при выборе контрагентов по договору. В данном деле суд приходит к следующему выводу: "ОАО не проявило достаточной осмотрительности в выборе контрагента по сделке. Счета-фактуры не подписаны руководителем ООО, что является нарушением императивных требований статьи 169 НК РФ и не позволяет обществу возместить налог на добавленную стоимость. Доказательств,

опровергающих изложенные обстоятельства, ОАО не представлено".

Федеральный арбитражный суд Московского округа в Постановлении от 02.02.2006, 01.02.2006 N КА-А40/83-06 занял сторону налогового органа ввиду того, что налогоплательщик не проявил необходимую осторожность и осмотрительность в выборе контрагентов, некоторые из которых, как выяснилось в ходе проверки, не находятся по своим адресам, а один из них в реестре налогоплательщиков не значится.

Однако при этом некоторые суды считают, что факт нарушения третьим лицом своих налоговых обязательств сам по себе не является основанием для вывода об отсутствии должной осмотрительности и осторожности со стороны налогоплательщика. Данное обстоятельство без доказательств того, что налогоплательщику было известно или могло быть известно о таких нарушениях со стороны третьего лица, еще не свидетельствует о неправомерности действий налогоплательщика <3>.

Данные подходы разделил и ВАС РФ, который разъяснил, что в случае доказанности действий организации или индивидуального предпринимателя без должной осмотрительности и осторожности, а также факта того, что им должно было быть известно о нарушениях, допущенных контрагентом, суд может признать необоснованной налоговую выгоду, полученную от совершения конкретной сделки в виде уменьшения размера налоговой обязанности вследствие, в частности, уменьшения налоговой базы, получения налогового вычета, налоговой льготы, применения более низкой налоговой ставки, а также получение права на возврат (зачет) или возмещение налога из бюджета <4>.

Таким образом, для обеспечения безопасности будущей сделки прежде всего следует собрать предварительные сведения о предполагаемом партнере:

- организационно-правовая форма партнера, предусмотренная учредительными документами (поскольку все они имеют разную степень ответственности);

- подтверждаются ли сведения о государственной регистрации партнера (поскольку возможно, что это лицо является фиктивным);

- разрешена ли подобная деятельность в уставе партнера, имеется ли лицензия на осуществление данного вида деятельности (так как в противном случае сделка может быть признана недействительной).

Далее необходим сбор и анализ общей информации о партнере:

- финансово-экономической (производится экспресс-анализ бухгалтерского баланса на последнюю отчетную дату. Например, если размер оборотных активов превышает размер краткосрочных пассивов, то такое предприятие можно признать финансово устойчивым. Могут рассчитываться такие финансовые показатели, как рентабельность производства, финансовые коэффициенты (автономии, текущей ликвидности, покрытия и их основные тенденции в течение ряда лет));

- организационной (количество работающих, структура фирмы, система управления и степень самостоятельности, наличие филиалов, территориальный охват деятельности);

- рыночной (контролируемая доля рынка, имидж фирмы, возможность конкуренции с

ней, постоянные контрагенты);

- специфической (наличие теневого оборота, участие в нелегальных сделках, связи с преступными группировками и т.п.);

- сведения об управленческом персонале фирмы (образование, наличие судимости, компетентность, деловая репутация).

После сбора общей информации о предполагаемом деловом партнере необходимо проанализировать полученные сведения и определить степень его надежности как потенциального контрагента. Для этого используются методы рейтинговой оценки либо принимается решение на основании положительной информации по всем (или большинству) аспектам деятельности потенциального партнера.

В самом общем виде все потенциальные партнеры по степени надежности могут быть разделены на три группы:

Первая группа - наиболее надежные партнеры. Вся собранная информация по названным критериям является положительной. Это позволяет сделать вывод о том, что данный партнер выполняет свои обязательства и имеет высокую исполнительскую дисциплину по совершаемым сделкам.

Вторая группа - партнеры средней степени надежности. Информация свидетельствует, что в большинстве случаев партнер старается выполнять свои обязательства, хотя имели место единичные нарушения условий сделок.

Третья группа - контрагенты с низкой степенью надежности. Они, как правило, не выполняют взятых на себя обязательств, используют нелегальные методы в своей деятельности, зачастую занимаются запрещенными видами деятельности либо связаны с организованными преступными группировками.

Отнесение потенциального партнера к одной из групп позволяет в конце данного (предварительного) этапа принять одно из возможных решений:

- отказ от подписания договора с данным контрагентом;

- подписание протокола о намерениях (это может быть использовано в случае, когда собранной информации оказалось недостаточно и необходима дополнительная проверка для определения надежности потенциального партнера);

- согласие на подписание договора.

Вопрос 2. ОСНОВНОЙ ЭТАП

Следующим этапом по обеспечению безопасности сделки должен стать процесс определения условий договора. После принятия решения о выборе контрагента стороны приступают к обсуждению условий соглашения, которые составляют содержание договора.

Договор считается заключенным, если между сторонами в требуемой в подлежащих случаях форме достигнуто соглашение по всем существенным условиям договора.

Следовательно, в первую очередь следует достичь согласия по всем существенным условиям договора. При этом существенными являются условия о предмете договора, условия, которые названы в законе или иных правовых актах как существенные или необходимые для договоров данного вида, а также все те условия, относительно которых по заявлению одной из сторон должно быть достигнуто соглашение (см. п. 1 ст. 432 ГК РФ).

Существенные условия необходимы и достаточны для заключения договора и требуют согласования сторон, например предмет договора, цена товара или оценка залога.

Далее (при необходимости) можно согласовать обычные условия (например, при заключении договора аренды автоматически вступает в действие условие, предусмотренное ст. 211 ГК РФ, в соответствии с которым риск случайной гибели или случайного повреждения имущества несет его собственник, т.е. арендодатель) и случайные условия, которые изменяют либо дополняют обычные условия. Например, если при согласовании условий договора купли-продажи стороны не решили, каким видом транспорта будет доставлен товар покупателю, то договор считается заключенным и без этого случайного условия.

Следует четко оговаривать в договоре распределение между сторонами обязанностей по транспортировке продаваемого товара и по его страхованию на период транспортировки. Это обусловлено тем, что цена товара прямо зависит от того, кто оплачивает расходы по транспортировке: продавец или покупатель.

Нельзя забывать, что сделка, совершенная с нарушением нормативных предписаний, ничтожна, т.е. недействительна с момента совершения (см. ст. 168 ГК РФ).

Таким образом, именно от того, насколько правильно стороны согласуют все необходимые по закону условия, зависит ее "легальность" в будущем, т.е. главной гарантией обеспечения безопасности на основном этапе заключения договора является определение всех его существенных условий. Разработку текста договора целесообразнее осуществлять с помощью собственных специалистов, поскольку в этом случае в проекте полнее можно отразить собственные интересы, что позволит повысить степень безопасности сделки. При этом следует учитывать, что каждый договор должен иметь ряд обязательных элементов.

Так, договор купли-продажи включает:

- преамбулу, в которой указывается наименование договора (например, купли-продажи), место и время его заключения, наименование сторон;

- основную часть, т.е. предмет договора (количество товара), цена товара, качество, базисные условия поставки, скидки с цены, форма платежа, срок поставки, односторонний отказ от договора, маркировка, упаковка товара, сдача-приемка товара, ответственность сторон. Сюда же относятся общие условия договора: порядок рассмотрения споров и форс-мажорные обстоятельства;

- заключительную часть - юридические адреса сторон, все приложения, подписи сторон.

Согласовываем форму расчетов. Значительные возможности для противодействия угрозам безопасности сделки кроются в выборе формы расчетов между

контрагентами, поскольку весьма распространены правонарушения (в том числе и преступления) именно в сфере расчетных отношений.

Наиболее надежной считается наличная форма расчетов, однако она не всегда возможна, так как закон ограничивает ее применение. Предельный размер расчетов наличными деньгами между юридическими лицами установлен Указанием Банка России от 20.06.2007 N 1843-У и составляет 100 тыс. руб. При этом указанное ограничение действует в рамках одного договора, заключенного между указанными лицами. Безналичные же расчеты могут осуществляться с помощью платежных поручений, аккредитивной формы расчетов, платежных требований-поручений, а также с помощью различного рода ценных бумаг, например векселей и чеков (см. ст. 862 ГК РФ). Необходима тщательная проверка наличия денег на счете контрагента и подлинности ценных бумаг.

Применяя в настоящее время наиболее распространенную в России форму безналичных расчетов - платежные поручения, следует учитывать, что они должны приниматься от плательщика к исполнению только при наличии средств на счете.

При использовании платежного требования-поручения поставщик для большей гарантии может внести в условия договора акцепт. Поручение акцептуется банком, что гарантирует при поступлении платежного требования-поручения списание средств со счета контрагента. Для этого необходимо два условия:

1) наличие в договоре пункта о форме и порядке оплаты (т.е. форма - платежное требование-поручение, порядок - с использованием акцепта);

2) наличие документа о согласии банка произвести акцепт по данному договору.

Наиболее безопасной для предпринимателей формой безналичных расчетов в современных российских условиях является аккредитивная форма. В этом случае гарантия оплаты обеспечивается предварительным депонированием денежных средств покупателя на банковском счете продавца (поставщика). При условии выполнения продавцом требований аккредитива (например, осуществление поставки товаров в срок и представление соответствующих транспортных документов) банк продавца производит списание средств в его пользу.

При использовании в расчетах векселей (т.е. безусловного денежного обязательства векселедателя уплатить при наступлении срока определенную сумму владельцу векселя) следует учитывать наличие различных форм злоупотреблений в сфере вексельного обращения и отдавать предпочтение векселям наиболее надежных субъектов хозяйствования. В настоящее время такими являются, например, Газпром, некоторые банки (в частности, Сбербанк России).

Следует также учитывать, что надежность векселя повышается в случае его аваля Минфином России, субъектом Российской Федерации, банком либо акцепта (согласие плательщика оплатить вексель в срок посредством проставления на векселе собственноручной подписи). Наконец, если вексель передается с помощью индоссамента (передаточной надписи), то следует удостовериться, что индоссамент был надлежаще оформлен всеми держателями векселя.

После того как все условия договора согласованы, необходимо еще раз проверить содержание договора в целом и на предмет отсутствия в договоре пунктов,

запрещенных законом, например условий, противоречащих законодательству о защите конкуренции <5> (о разделе рынков, соглашении фирм и т.п.), поскольку их наличие может привести к санкциям против заключивших договор лиц.

Вопрос 3. ЗАКЛЮЧИТЕЛЬНЫЙ ЭТАП

На заключительном этапе производится подписание договора. Здесь также следует быть очень внимательным. Договор может заключаться в устной или письменной форме (см. ст. 158 ГК РФ). Следует иметь в виду, что сделки, которые должны совершаться в простой письменной форме, - это сделки юридических лиц между собой и с гражданами. Для некоторых же видов сделок требуется нотариальное удостоверение либо государственная регистрация. Для того чтобы сделка не могла быть признана недействительной, следует соблюдать требуемую законодательством форму. Так, например, весьма часто в предпринимательской деятельности возникает нехватка каких-либо ресурсов (финансовых, товарных). В этом случае сторона вынуждена прибегать к займу, который оформляется соответствующим договором займа. Договор займа должен быть заключен в простой письменной форме тогда, когда заимодавец является юридическим лицом либо сумма договора, заключаемого между гражданами, превышает не менее чем в 10 раз минимальный размер оплаты труда, установленный законодательством (ст. 808 ГК РФ). В остальных случаях этот договор не требует даже простой письменной формы.

Затем стороны приступают к подписанию договора. В процедуре подписания договора необходимо проверить правоспособность лица, которое подписывает договор с противоположной стороны. Часто способом, который применяют недобросовестные контрагенты для ухода от выполнения обязательств, является заявление о том, что лицо, подписавшее договор с их стороны, соответствующих полномочий не имело.

Договор должен быть подписан директором либо полномочными лицами, определенными уставом (например, "Договор заключен между ООО "Ромашка" в лице директора фирмы Василькова В.В., действующего на основании Устава..."). Если договор подписан лицом, у которого отсутствуют полномочия на подписание в уставных документах, то это лицо должно действовать на основании доверенности (см. гл. 10 ГК РФ), подписанной руководителем этой фирмы. В противном случае может иметь место недобросовестность контрагента, так как данный договор может быть признан недействительным в судебном порядке.

<1> См. Постановление ФАС Восточно-Сибирского округа от 10.03.2005 N А33-7618/04-С2-Ф02-825/05-С2.

<2> См. Постановление ФАС Восточно-Сибирского округа от 22.12.2003 N А33-6135/03-С2-Ф02-4458/03-С2.

<3> См. Постановление ФАС Поволжского округа от 21.12.2004 N А55-6275/04-11.

<4> Постановление Пленума ВАС РФ от 12.10.2006 N 53.

<5> Федеральный закон от 26.07.2006 N 135-ФЗ "О защите конкуренции", ст. ст. 14.32, 14.33 КоАП РФ.

Практическое занятие 7

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ КУПЛИ-ПРОДАЖИ ПРЕДПРИЯТИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ СЕТИ ИНТЕРНЕТ

Учебные вопросы:

1. Сделки в Интернете.
2. Правовое регулирование купли-продажи предприятия в Интернете.
3. Особенности купли-продажи интернет-магазина

Введение

На продажу в настоящее время выставляются не только предприятия в стадии угасания и банкроты, но и предприятия, способные приносить доход, не обремененные долгами.

"Бизнес на продажу" - уже не только процесс, но и товар, для продажи которого создаются специальные фирмы, представляющие интересы продавца и покупателя на всех стадиях - от консалтинга и проверки прав собственности продавца до переговоров и оформления документов о продаже.

В идеальном случае данная фирма - это некое подобие торговой площадки, т.е. место встреч продавцов и покупателей, обеспечивающее первых достаточным уровнем конфиденциальности, вторых - информацией о предложении готового бизнеса, и тех и других - гарантированным сервисом (независимые оценщики, эксперты, консультанты, предоставление места для проведения переговоров и т.п.).

Стандартная процедура покупки бизнеса предусматривает внесение покупателем залога, после чего он получает возможность в течение двух-трех месяцев руководить предприятием. Если доходы, полученные от покупки бизнеса, оказываются меньше заявленных, сделка расторгается и покупатель получает аванс обратно. Иными словами, как продавцы, так и посредники не заинтересованы завышать свои доходы - в этом случае они просто "подарят" потенциальным покупателям два-три месяца работы на объекте.

Вопрос 1. СДЕЛКИ В ИНТЕРНЕТЕ

Последние годы наиболее динамично развивающимся сегментом экономической активности хозяйствующих субъектов во всем мире становится электронный бизнес (или, как его еще называют, электронная коммерция, электронная экономическая деятельность).

Следует отметить, что в широком смысле электронная хозяйственная деятельность представляет собой совокупность процессов, направленных на перераспределение

товаров (работ, услуг) в ходе производства хозяйствующими субъектами предпринимательской деятельности, и процессов, направленных на обеспечение такого перераспределения, формирующихся в ходе осуществления хозяйствующими субъектами непредпринимательской деятельности, тесно связанной с обеспечением предпринимательской деятельности, в электронной форме с использованием современных информационных технологий. При этом в качестве экономического инструмента осуществления названных процессов выступает сеть "Интернет".

Сделки в Интернете совершаются в виртуальном пространстве, которое отличается от реального физического пространства. В силу этого, рассматривая вопрос о купле-продаже предприятия в глобальной компьютерной сети, следует указать четыре основных признака сделки в Интернете [1]:

- сделка в Интернете обладает качеством юридического факта, представляющего собой действие граждан и юридических лиц, совершение которого приводит к установлению, изменению или прекращению гражданских прав и обязанностей;

- сделка в Интернете - это волевое действие. Его совершение предполагает наличие определенного уровня сознания и воли у субъекта, которые позволяют данному лицу руководить своими действиями и отдавать отчет в своих поступках;

- сделка в Интернете представляет собой действие, направленное волей и имеющее своей целью достижение субъективно предполагаемого участниками сделки определенного результата;

- сделка в Интернете - это правомерное действие ее участников, т.е. действия участников сделки должны находиться в сфере дозволенности или в сфере незапрещенности законом. Сделка, которая не отвечает этим требованиям, недействительна (ст. 168 ГК РФ).

Основываясь на изложенном был сделан вывод, что сделки в Интернете по исследованным четырем признакам не отличаются от сделок вне сети Интернет. С данным выводом трудно не согласиться. Иными словами, сделка, в частности купля-продажа предприятия, совершаемая в Интернете, должна отвечать требованиям, установленным гражданским законодательством. Но для совершения сделки в Интернете необходимо использование специальных программных и аппаратных средств, что в других обстоятельствах обычно не требуется.

Вопрос 2. ПРАВОВОЕ РЕГУЛИРОВАНИЕ КУПЛИ-ПРОДАЖИ ПРЕДПРИЯТИЯ В ИНТЕРНЕТЕ

По нашему мнению, для рассмотрения вопроса нормативного урегулирования купли-продажи предприятия в сфере сети "Интернет" представляется целесообразным проанализировать сами понятия "электронная коммерция" и "электронная торговля".

Типовой закон Комиссии Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) об электронной торговле 1996 г. [2] трактует понятие "electronic commerce" как договорные, в том числе не носящие предпринимательский характер, так и внедоговорные отношения торгового

характера, осуществляемые с использованием электронных средств. Действие данного понятия распространяется в п. 2 ст. 1 Директивы Европейского Парламента и Совета от 20 июля 1998 г. N 98/48/EC о внесении поправок в Директиву 98/34/EC на любую услугу, предоставляемую на расстоянии за вознаграждение с использованием электронных средств по персональному запросу ее получателя [3]. Всемирная торговая организация (ВТО) определяет понятие "electronic commerce" как распределение, маркетинг, продажу или поставку товаров и услуг с помощью электронных средств связи [4].

Под электронной торговлей, как правило, понимаются сделки купли-продажи, совершенные с использованием средств электронного документооборота, или совокупность действий, направленных на заключение таких сделок. Одни специалисты считают понятия "электронная коммерция" и "электронная торговля" эквивалентными (равными по объему) [5], другие специалисты полагают, что электронная коммерция - это любая форма бизнес-процесса, в котором взаимодействие между субъектами происходит электронным образом и сопровождается снабжением ресурсами или физической доставкой продукции. Электронная торговля, которая касается процесса продаж, является частью электронной коммерции и наиболее активно развивается в сети Интернет [6].

Изложенное позволяет сделать вывод о необходимости скорейшего разрешения проблемы научной разработки и унификации терминологии в сети Интернет, а также единообразного толкования основных понятий и институтов в рассматриваемой сфере.

При разработке и принятии Гражданского кодекса РФ (далее - ГК РФ) законодатель принципиально отказался от использования термина "коммерция" для определения деятельности, направленной на извлечение прибыли. Для обозначения базового понятия в сфере имущественных и связанных с ними личных неимущественных отношений, на основе которого во многом и строится правовое регулирование, в российском гражданском законодательстве используется понятие "предпринимательская деятельность". Термин "экономическая деятельность" - в ч. 1 ст. 8 и в ст. 34 Конституции Российской Федерации. Следует отметить и то обстоятельство, что в ст. 3 Налогового кодекса РФ содержится термин "экономическая деятельность".

Анализ норм ст. 34 Конституции Российской Федерации позволяет сделать вывод, что, во-первых, понятия "предпринимательская деятельность" и "экономическая деятельность" различаются по своему объему, а во-вторых, понятие "экономическая деятельность" шире понятия "предпринимательская деятельность", ибо последняя рассматривается Конституцией Российской Федерации в качестве одного из видов экономической деятельности. Кроме того, Конституция Российской Федерации закрепляет за каждым гражданином России и иными лицами, законно находящимися на ее территории, право свободно вести экономическую деятельность и специально выделяет предпринимательскую деятельность в качестве главного ее вида.

По нашему мнению, необходимо закрепление в российском законодательстве термина "электронная экономическая деятельность", под которым следует понимать предпринимательскую деятельность, а также тесно связанную с ней не запрещенную законом экономическую деятельность, осуществляемую в электронной форме, т.е. с использованием современных коммуникационных средств, в том числе в

информационной среде Интернет.

Вместо термина "электронная коммерция" целесообразно использовать понятие "электронная экономическая деятельность" (экономическая деятельность, осуществляемая в электронной форме с использованием современных коммуникационных средств).

Согласно нашей точки зрения, электронная экономическая деятельность - это сфера деловой деятельности, осуществляемая в электронной форме и включающая электронную торговлю, электронный документооборот и электронную систему платежей. Под электронной торговлей должны подразумеваться заключение и исполнение сделок с использованием электронных средств, а также приобретение и осуществление иных прав и обязанностей с использованием электронных средств в сфере предпринимательской и иной не запрещенной законом экономической деятельности.

Необходимо отметить, что термин "электронные средства" содержится в определении понятий "электронная торговля" и "электронные сделки". По нашему мнению, следует согласиться с той точкой зрения, что электронные средства - это "аппаратные и (или) программные технические средства, используемые для создания, хранения, а также передачи и (или) приема электронных документов посредством электронной связи" [7]. В частности, абз. 4 ст. 3 Федерального закона от 10 января 2002 г. N 1-ФЗ "Об электронной цифровой подписи" (в ред. от 8 ноября 2007 г.) (далее - Закон об электронной цифровой подписи) дает определение средствам электронной цифровой подписи.

По нашему мнению, центральным элементом понятийного аппарата, применяемого при регламентации электронных сделок, является понятие "электронный документ". Следует отметить, что согласно п. 3 ст. 11 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом. Термин "электронный документ" используется в российском законодательстве, например в Законе об электронной цифровой подписи. Некоторые авторы используют для обозначения анализируемого понятия другие термины, например, предлагается закрепить в законодательстве понятие "компьютерный (машинный) документ", под которым должны пониматься документы, создаваемые, хранимые и/или предоставляемые адресату с помощью компьютерной техники, и документы, переданные современными электронными средствами передачи информации, или ввести понятие "машинный документ".

В проекте федерального закона N 310163-4 "Об электронной торговле", внесенного депутатом В.Я. Комиссаровым в Государственную Думу Федерального Собрания, используется понятие "электронное сообщение", под которым понимается "информация, преобразованная в форму, пригодную для передачи и (или) хранения с использованием компьютерных устройств", но не предусмотрен термин "электронный документ". По нашему мнению, принятие данного понятия противоречит действующему российскому законодательству, которое предусматривает возможность совершения сделки в письменной форме исключительно путем составления документа (п. 1 ст. 160 ГК РФ). Следовательно, необходимо использовать понятие электронного документа, представленное в ст. 3 Закона об электронной цифровой подписи, т.е.

электронный документ - это документ, в котором информация представлена в электронно-цифровой форме. Электронно-цифровая форма электронного документа по своим юридическим последствиям в законодательстве Российской Федерации приравнивается к письменной форме. Данный вывод подтверждается положением ст. 158 ГК РФ, указывающей, что сделки совершаются в устной или письменной форме, а также ст. 434 ГК РФ, закрепляющей, что договор в письменной форме может быть заключен в том числе путем обмена документами посредством электронной связи. Реквизиты, в которых воплощается электронно-цифровая форма документа, имеют свои особенности. В электронном документе проставление собственноручной подписи и скрепление его печатью невыполнимы. Согласно п. 2 ст. 160 ГК РФ допускается использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи в случаях и порядке, предусмотренных законом, иными правовыми актами или соглашением сторон. При совершении сделки в письменной форме, в частности купли-продажи предприятия, в Интернете для электронного документа наиболее подходит электронно-цифровая подпись, которая представляет собой набор символов, генерируемых специальной компьютерной программой по специальному алгоритму в результате совмещения текста подписываемого документа и личного кода подписывающего документ лица.

Электронно-цифровая подпись обладает двумя свойствами:

- может быть воспроизведена только одним лицом, а подлинность ее может быть удостоверена многими;

- неразрывно связана с конкретным документом. Электронно-цифровая подпись увязывает в одно целое содержание документа и закрытый ключ подписывающего, делая невозможным изменение документа без нарушения подлинности этой подписи [8].

Использование электронно-цифровой подписи возможно только при наличии в компьютерной системе возможностей, обеспечивающих идентификацию подписей, а также соблюдение установленного режима их использования. Право удостоверять идентичность электронно-цифровой подписи реализуется на основании лицензии.

В соответствии с п. 2 ст. 4 Закона об электронной цифровой подписи участник информационной системы может быть одновременно владельцем любого количества сертификатов ключей подписей. При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи. В связи с этим возникают вопросы о необходимости наличия у юридического лица одновременно нескольких электронно-цифровых подписей для подписания электронных документов, порождаемых в рамках различных отношений, также о соответствии этому требованию в ситуации смешанного договора (ст. 421 ГК РФ). В итоге потребуется проведение владельцем электронно-цифровой подписи анализа подписываемых электронных документов на предмет соответствия электронно-цифровой подписи конкретным правоотношениям или использования для одного электронного документа нескольких электронно-цифровых подписей по видам отношений [9].

Согласно ст. 1 Закона об электронной цифровой подписи действие данного нормативного документа распространяется на отношения, возникающие при

совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. В соответствии со ст. 19 данного Закона содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, может заверяться согласно нормативным правовым актам или соглашениям сторон электронной цифровой подписью уполномоченного лица. В случаях, установленных законами и иными нормативными правовыми актами Российской Федерации или соглашением сторон, электронная цифровая подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью. Следовательно, договор продажи предприятия, заключенный в электронном виде, должен расцениваться как заключенный в надлежащей форме.

Необходимо отметить, что для развития гражданского оборота, осуществляемого с использованием Интернета, необходим закон, нормы которого будут посвящены регулированию отношений, связанных с совершением сделок и с заключением договоров с использованием электронных средств. Такой законопроект N 27813-3 "О сделках, совершаемых при помощи электронных средств (об электронных сделках)" был внесен депутатом Государственной Думы Федерального Собрания С.А. Прощиным. Согласно данному законопроекту сделки, которые в соответствии с законодательством Российской Федерации должны быть нотариально удостоверены или подлежат государственной регистрации, не могут быть совершены с использованием электронных средств.

По нашему мнению, отсутствие системы источников и фрагментарность законодательства свидетельствуют об отсутствии правовой базы для осуществления электронных сделок в том объеме, который позволяет осуществлять уровень развития технологии. Необходима выработка единого понятийного аппарата. Без решения этой задачи будут затруднены разработка необходимых нормативных правовых актов и совершенствование действующего законодательства, призванного регулировать общественные отношения в информационной среде сети Интернет.

Вопрос 3. ОСОБЕННОСТИ КУПЛИ-ПРОДАЖИ ИНТЕРНЕТ-МАГАЗИНА

Представляет интерес вопрос о купле-продаже такого предприятия, как интернет-магазин. Учитывая п. 1 ст. 492 ГК РФ, речь идет о незаконном предпринимательстве, если в качестве интернет-магазина деятельность ведет не имеющее статуса индивидуального предпринимателя физическое лицо, на которое зарегистрировано доменное имя. Данное физическое лицо может быть привлеченным к ответственности, вплоть до уголовной, согласно ст. 171 Уголовного кодекса РФ.

Состав при купле-продаже интернет-магазина отличается от состава предприятия при купле-продаже в обычном порядке. Необходимо отметить, что существование интернет-магазина невозможно без функционирования интерактивного ресурса в сети (web-сайта), для существования которого необходимо несколько составляющих: доменное имя, сервер (хостинг), наполнение или контент web-сайта (текстовое,

графическое или иное содержание сайта) и система управления сайтом (Control Management System или CMS), а также некая совокупность узнаваемой и широко известной символики (бренд). Понятие "бренд" отсутствует в российском законодательстве. На наш взгляд, бренд интернет-магазина может включать и фирменное наименование, и коммерческое обозначение, и товарный знак (знак обслуживания). Также необходимо отметить сеть договорных связей с поставщиками тех товаров, которые предлагаются на сайте в Интернете.

Изложенные особенности интернет-магазина влекут необходимость особого порядка передачи прав на составляющие его объекты. Учитывая, что согласно п. 1 ст. 454 ГК РФ предметом купли-продажи может быть только вещь (товар), то о купле-продаже интернет-магазина не может идти речь, хотя на практике такая сделка осуществляется. Под куплей-продажей интернет-магазина предполагается передача прав на перечисленные объекты без ограничения срока такой передачи и без обязательства о возврате таких объектов первоначальному правообладателю [10].

В частности, передача прав на зарегистрированное доменное имя (регистрацию проводят специализированные организации-регистраторы в определенной доменной зоне) при отчуждении интернет-магазина должна быть зарегистрирована. Приобретатель интернет-магазина, не перерегистрировавший на себя доменное имя, может столкнуться с трудностями, например с невозможностью открыть соответствующую страницу в Интернете, если прежний владелец решит такую страницу заблокировать. На это было указано, например, в Постановлении ФАС Московского округа от 9 февраля 2005 г. по делу N КГ-А40/20-05. Суд отметил, что доступ к интернет-сайту, который размещен в сети под определенным доменным именем, имеет только администратор соответствующего доменного имени, который самостоятельно регистрирует индивидуальный пароль для доступа к информации о домене.

Что касается хостинга, то, если права владельца на доменное имя зарегистрированы и администрирование сайта осуществляется им самостоятельно, сайт может быть по выбору владельца размещен на любом сервере. Договор на хостинг прежнего владельца сайта прекращается, вместо него новый владелец заключает другой договор с определенным (по своему усмотрению) обладателем соответствующего сервера.

Фирменное наименование, являясь составной частью бренда в соответствии с п. 1 ст. 1474 ГК РФ, используется в качестве средства индивидуализации. Согласно п. 2 ст. 1474 ГК РФ распоряжение исключительным правом на фирменное наименование (в том числе путем его отчуждения или предоставления другому лицу права использования) не допускается. На основании п. 2 ст. 1476 ГК РФ фирменное наименование может быть включено в товарный знак или знак обслуживания. Принимая во внимание норму ГК РФ, запрещающую отчуждение прав на фирменное наименование, по нашему мнению, права на товарный знак, включающий в качестве составной части фирменное наименование организации-правообладателя, также не подлежат передаче.

В соответствии с п. 4 ст. 1539 ГК РФ коммерческое обозначение переходит от правообладателя к другому лицу только в составе предприятия. Следовательно, приобретатель интернет-магазина должен заключить с правообладателем договор купли-продажи предприятия, для индивидуализации которого используется

соответствующее коммерческое обозначение. При заключении данного договора должны быть соблюдены все правила о форме и регистрации такого договора, порядке его заключения и формировании его условий, которые предусмотрены гл. 30 ГК РФ.

Необходимо отметить, что право использования товарного знака передается путем заключения лицензионного договора на определенный срок либо путем заключения договора на отчуждение данного права. Данный договор подлежит государственной регистрации. Дизайнерское решение сайта также является охраняемым объектом авторских прав. Передача исключительного права на данное произведение осуществляется в общем порядке, предусмотренном законодательством. Исключительные права на произведение могут быть переданы полностью на их отчуждение согласно ст. 1285 ГК РФ либо по лицензионному договору в соответствии со ст. 1286 ГК РФ на установленный период времени. Система управления сайтом, представляя собой программу для ЭВМ, также охраняется законодательством в указанном качестве. Если новый владелец интернет-магазина пренебрегает приобретением у прежнего хозяина пригодной для управления конкретным сайтом системы управления, он не сможет внести какие-либо изменения в контент сайта.

Относительно товарного "наполнения" сайта следует отметить, что ввиду физического отсутствия товара в интернет-магазине новому владельцу могут передаваться только договорные связи с поставщиками, что происходит путем уступки прав требований по соответствующим договорам прежних их участников приобретателю интернет-магазина.

Из изложенного следует, что для передачи прав на интернет-магазин недостаточно заключить один договор - в данном случае речь идет об отчуждении комплекса прав, составляющих такое явление правовой реальности, как интернет-магазин.

Правовая база, регулирующая куплю-продажу интернет-магазина, весьма незначительна. Поэтому необходимо развитие соответствующего законодательства, приспособленного к современным реалиям и обеспечивающего защищенность в новых сферах деятельности.

Список литературы

1. Малахов С.В. Гражданско-правовое регулирование отношений в глобальной компьютерной сети Интернет: Дисс. М.: РГБ, 2002. С. 114.

2. Типовой закон Комиссии Организации Объединенных Наций по праву международной торговли (ЮНСИТРАЛ) об электронной торговле 1996 г.: рекомендован резолюцией Генеральной Ассамблеи ООН от 16 декабря 1996 г. N 51/162 // Комиссия ООН по праву международной торговли: Ежегодник. 1996. Т. XXVII. Нью-Йорк: Организация Объединенных Наций, 1998. С. 319 - 323.

3. Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations // Official Journal of the European Communities L 217, 05/08/1998. P. 0018 - 0026.

4. Перечень терминов, краткое описание процедур и договоренностей, принятых в рамках ВТО // Всемирная торговая организация: документы и комментарии / Под ред. С.А. Смирнова. М., 2001. С. 126.

5. Маршавин Р.А., Ляпунов С.И. Глобальный бизнес и информационные технологии: современная практика и рекомендации / Под ред. В.М. Попова. М.: Финансы и статистика, 2001. С. 55.

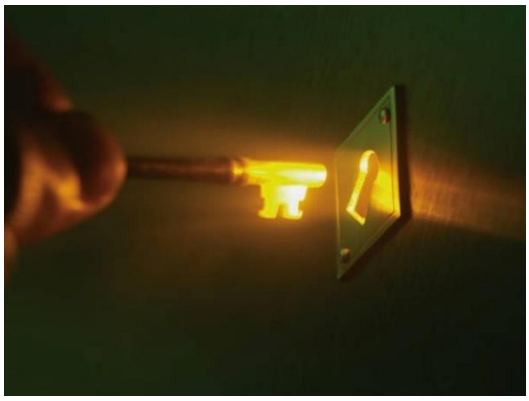
6. Скородумов Б.И. Стратегия информационной безопасности в Интернете: Сб. трудов X Международной научной конференции "Информатизация правоохранительных систем". М., 2001. С. 72.

7. Кареев Я.А. Правовое регулирование использования электронных документов в договорных отношениях: анализ основных понятий // Актуальные проблемы международного частного и гражданского права: Сб. статей к 80-летию В.А. Кабатова. М.: Статут, 2006. С. 141.

8. Гарибян А. Электронная цифровая подпись: правовые аспекты // Российская юстиция. 1996. N 11. С. 12; Вершинин А.П. Электронный документ: правовая форма и доказательство в суде. М., 2000. С. 66 - 71.

9. Шамраев А. Электронная подпись: вопросов пока больше, чем ответов // Коллегия. 2002. N 2. С. 14, 15; Соловяненко Н. Совершение сделок путем электронного обмена данными (принципы правового подхода) // Хозяйство и право. 1997. N N 6 - 7.

10. Яковлева О.А. Интернет-магазин: правовая реальность // Финансовые и бухгалтерские консультации. 2008. N 4.



ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

(учебно-методическое пособие)

В настоящее время, в условиях выхода экономики государства из периода депрессии, достижение стабильности функционирования субъектов предпринимательской и других видов деятельности является наиболее актуальной и важной задачей. Для решения её немаловажную роль играет обеспечение экономической безопасности этих субъектов.

Предназначено для преподавателей и студентов вузов экономических специальностей, а также специалистов по экономической безопасности, менеджеров, руководителей компаний.

СОДЕРЖАНИЕ

Введение

Глава 1. Теоретические основы экономической безопасности предприятий

1.1. Экономическая безопасность. История вопроса

1.2. Концепция национальной безопасности

1.3. Критерии и показатели экономической безопасности национальной экономики

1.4. Оценка бизнеса на наличие угроз безопасности

1.5. Первые шаги по обеспечению безопасности бизнеса

Глава 2. Процесс обеспечения экономической безопасности на региональном уровне

2.1. Система показателей и индикаторов экономической безопасности в регионе

2.2. Модель конкурентной среды М. Портера

2.3. Алгоритм обеспечения экономической безопасности в регионе

2.4. Виды недобросовестной конкуренции

Глава 3. Деятельность по обеспечению экономической безопасности предприятий

3.1. Обеспечение экономической безопасности предприятия. Основные определения

3.2. Причины дестабилизации экономической безопасности

3.3. Классификация угроз

3.4. Механизм реализации угроз

3.5. Задачи экономической безопасности

Глава 4. Финансово-хозяйственная деятельность предприятия

4.1. Принципы построения системы безопасности предприятия

4.2. Классификация элементов финансово-хозяйственной деятельности

4.3. Информация о финансово-хозяйственной деятельности предприятия, как основа безопасности

4.4. Финансовая диагностика экономической безопасности предприятия

Глава 5. Особенности экономической безопасности на предприятиях различных отраслей

5.1. Промышленные предприятия

5.2. Интернет и информационные системы

5.3. Строительство

5.4. Торговля

5.5. Транспорт и связь

5.6. Экономическая безопасность вузов

Глава 6. Построение системы экономической безопасности предприятия

6.1. Общие принципы

6.2. Создание и организационная структура служб безопасности предприятий

Глава 7. Применение систем безопасности в различных отраслях деятельности

7.1 Системы безопасности в торговле

7.2. Проверка и оценка потенциального бизнес-партнера

7.3. Система защиты коммерческого предприятия

7.4. Обеспечения комплексной безопасности на предприятиях электроэнергетики

7.5. Система информационной безопасности предприятия

7.6. Разработка и реализация политики безопасности предприятия

Глоссарий

Список литературы

ВВЕДЕНИЕ

В настоящее время, в условиях выхода экономики государства из периода депрессии, достижение стабильности функционирования субъектов предпринимательской и других видов деятельности является наиболее актуальной и важной задачей.

Для решения её немаловажную роль играет обеспечение экономической безопасности этих субъектов.

На экономический рост предприятия может оказывать влияние различные факторы. Экономический рост тесно связан с проблемами расширенного воспроизводства, более того, экономический рост является концентрированным выражением и способом разрешения проблем воспроизводства.

Экономический рост – тенденция изменения совокупных показателей развития предприятия за определенный промежуток времени, обычно за год. Для характеристики экономического роста используются как общие, так и частные показатели.

Общим показателем динамики экономического роста обычно считается рост выручки, прибыли и рентабельности за определенный период времени. В качестве частных показателей используются производительность труда, эффективность производства и т. д. Экономическая ситуация в государстве, кроме ряда прочих факторов, находится в зависимости от способности соответствующих государственных органов обеспечить как экономическую безопасность государства, так и хозяйствующих субъектов - предприятий, В то же время хозяйствующие субъекты, регионы страны, предприятия различных отраслей экономики должны прилагать собственные усилия для обеспечения своей экономической безопасности Экономическая безопасность - одна из составляющих обще го понятия «безопасность». Любой ущерб рано или поздно может получить оценку в денежном выражении, то есть может быть, выделена чисто экономическая составляющая ущерба.

В нашем государстве принят закон № 2446-1 «О безопасности» от 5 марта 1992 года.

Настоящий Закон закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

За рубежом проблеме безопасности бизнеса традиционно придается большее значение, так как опыт хозяйствования в условиях рыночной экономики у развитых зарубежных государств гораздо богаче, нежели у России. Это объясняется тем, что российская экономика отличается от стабильно и поступательно развивавшихся экономик развитых стран.

Руководитель предприятия (фирмы), предприниматель, осуществляющие свою деятельность в условиях рыночной экономики, испытывают ежедневный пресс со стороны конкурентов в борьбе за новых потребителей, за новые рынки сбыта, за качество выпускаемой продукции и оказываемых услуг.

Соревнование конкурентов вынуждает их постоянно заботиться о повышении эффективности производственно-хозяйственной и маркетинговой деятельности, снижении затрат, защите своих коммерческих секретов, способных за счет увеличения производительности и лучшего управления обеспечить стабильную финансовую устойчивость предприятия, что в свою очередь определяет их экономическую безопасность

Задачи курса:

✓ определение понятия и сущности экономической безопасности;

✓ определение основных задач в области обеспечения национальной безопасности Российской Федерации;

✓ характеристика основных критериев и показателей экономической безопасности;

✓ анализ основных показателей экономической безопасности России и регионов;

✓ выявление существующих и потенциальных угроз экономической безопасности России на современном этапе развития.

✓ формулировка принципов обеспечения экономической безопасности предприятий на основе моделирования отдельных процессов деятельности предприятий;

✓ исследование отраслевые особенности экономической безопасности предприятий;

✓ предложение механизма реализации комплексного подхода к организации деятельности по обеспечению экономической безопасности предприятий;

✓ обозначение направления развития деятельности по обеспечению экономической безопасности предприятий;

✓ формирование мотивации к созданию системы единого алгоритма действий в случае возникновения внешней и внутренней опасности.

Целевая аудитория курса:

✓ Владельцы предприятий и организаций;

✓ Руководители служб безопасности;

✓ Руководители предприятий и организаций;

✓ Управляющие различных уровней, специалисты в области безопасности, управления, экономики, и финансов, учета, аудита, контроля.

Скорее всего, многие согласятся с тем, что совершенно безразлично, будет ли предприятие разорено бандитами, вымогателями, штрафами налоговой инспекции, либо в результате недобросовестных действий деловых партнеров, конкурентов или собственного персонала. В любом случае оно может прекратить свое существование. Следовательно - речь надо вести об обеспечении безопасности деятельности организации.

Обеспечение безопасности необходимо для любых организаций, независимо от форм их собственности, начиная от государственных организаций и заканчивая маленькой палаткой, занимающейся розничной торговлей. Различие будет состоять лишь в том, какие средства и методы и в каком объеме требуются.

Конечно, о чем бы мы ни говорили - какие меры безопасности ни рассматривали, так или иначе, все направлено на обеспечение экономической стабильности в деятельности предприятия. Однако, достижение этой стабильности невозможно без анализа всех сторон деятельности предприятия.

В настоящее время положение дел в вопросах обеспечения безопасности и устойчивого функционирования хозяйственно-финансовых процессов в сфере предпринимательства весьма и весьма сложное. Отставание в разработке законодательства, регулирующего область развивающегося предпринимательства, неразбериха в сфере правоприменения и абсолютная рассогласованность действий различных государственных институтов сопровождаются ростом коррупции и криминала.

В этих условиях криминализируется и сама предпринимательская деятельность. Ее цель – извлечение прибыли с использованием незаконных методов и средств. Применительно к трем основным сферам предпринимательства (торговля, финансы, производство) общими для них негативными проявлениями являются уклонение от налогов, недобросовестная конкуренция, обман партнеров и клиентов и другие.

Сложившаяся ситуация в сфере предпринимательства и особенно в сфере малого бизнеса остро ставит проблему обеспечения безопасности и защиты интересов предпринимательства.

Обеспечение безопасности бизнеса не является исключительной прерогативой какого-либо одного отдела, службы или группы лиц. Она должна поддерживаться всей внутренней структурой предприятия, начиная от руководства и заканчивая рядовыми работниками, всеми звеньями и структурами объекта.

Обеспечение безопасности не может быть одноразовым актом. Это непрерывный процесс, заключающийся в поиске, обосновании и реализации наиболее рациональных методов, способов и приемов обеспечения безопасности, своевременном выявлении потенциальных угроз безопасности объекта.

Безопасность может быть обеспечена лишь при комплексном использовании всего арсенала сил и средств защиты, а также понимания важности вопросов обеспечения безопасности во всех структурных подразделениях объекта. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм - **комплексную систему безопасности**, необходимым элементом которого является подготовка персонала и соблюдение им всех установленных правил по обеспечению безопасности.

Также комплексная система безопасности не может обеспечить требуемый уровень безопасности объекта без надлежащего уровня **управления системой безопасности**.

Управление безопасностью бизнеса (компании, фирмы, предприятия) - многоступенчатый процесс, включающий:

- ✓ анализ экономических и правовых особенностей бизнеса,
- ✓ оценка бизнеса,
- ✓ аудит системы безопасности,
- ✓ анализ затрат на обеспечение безопасности бизнеса,
- ✓ разработку стратегии обеспечения безопасности,
- ✓ реализацию стратегии обеспечения безопасности,
- ✓ мониторинг тенденций развития бизнеса с целью совершенствования средств и методов его защиты,
- ✓ обучение основам личной безопасности сотрудников предприятия,
- ✓ оказание юридической помощи и экономических консультаций в реализации проектов предпринимательства.

Что же следует понимать под безопасностью предприятия, из чего она собственно состоит, и какие вопросы требуют повышенного внимания?

Безопасность предприятия – это состояние его защищенности от негативного влияния внешних и внутренних угроз, дестабилизирующих факторов, при котором обеспечивается устойчивая реализация основных коммерческих интересов и целей уставной деятельности.

Подобная защищенность достигается применением комплекса мер правового, экономического, организационного, инженерно-технического и социально-психологического характера.

Существующее мнение о том, что безопасность - это, прежде всего, физическая защищенность, не совсем верно. Безопасность предпринимательской деятельности сегодня - это не только автомат и бронестекло автомобиля, а, прежде всего, это вычисление и всесторонний анализ угроз деятельности предприятия; прогноз и создание систем и мер защиты и минимизации коммерческих рисков.

Под **угрозой безопасности предприятия** следует понимать потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности. При этом угрозами считаются не только такие очевидные факты, как, например, посягательство на личность: грабеж, рэкет или физическое насилие, то есть те, которые носят явно криминальный характер, но и такие неочевидные как: недобросовестность деловых партнеров и некомпетентность персонала, необоснованные претензии налоговых либо правоохранительных органов и т.д.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

1.1. Экономическая безопасность. История вопроса

Экономическая безопасность - часть общей системы национальной безопасности страны. Она затрагивает практически все стороны жизни государства, общества, экономики. Ее развитие необходимо рассматривать в общем контексте формирования системы национальной безопасности государства.

С распадом системы государственной безопасности СССР была утрачена концептуальная, стратегическая и институционально-организационная основа защиты национально-государственных интересов России. Старая парадигма государственной безопасности с ее идеологией, особым пониманием национально-государственных интересов и системой стратегических приоритетов уже не могла соответствовать новым представлениям о структуре национальной безопасности.

Политические, социально-экономические, геополитические и международные изменения, происходящие в ходе реформирования постсоциалистического экономического пространства, носят фундаментальный характер и затрагивают весь комплекс отношений и структур в области национальной и международной безопасности. Если рассматривать их долговременные стратегические аспекты, то объективно складываются следующие элементы формирующейся в условиях перехода к рыночной экономике новой парадигмы:

- переход в системе международных отношений от концепции баланса сил к концепции баланса интересов;

- движение от идеологии и структур национальной безопасности конфронтационного типа в сторону моделей, основанных на отношениях партнерства и равноправного международного сотрудничества;

- дополнение принципа защиты территории принципом обеспечения безопасности личности.

В 1992 г. был принят закон Российской Федерации «О безопасности», определивший ее базовые понятия и элементы. В нем были сформулированы понятия безопасности, жизненно важных интересов, выявлена триада основных объектов безопасности (личность, общество, государство). В качестве основного субъекта обеспечения безопасности названо государство, действующее в этой области через органы законодательной, исполнительной и судебной ветвей власти. Угрозы безопасности определены как совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества, государства. Разделены реальные и потенциальные угрозы объектам безопасности, исходящие от внутренних и внешних источников опасности.

В законе определено, что безопасность обеспечивается проведением единой государственной политики в этой области, системой мер экономического, политического, организационного и иного характера, адекватно отражающих угрозы жизненно важным интересам личности, общества, государства в целом.

В качестве основных принципов обеспечения безопасности законом от 1992 г. определены:

-законность;

- соблюдение баланса жизненно важных интересов личности, общества, государства; взаимная ответственность личности, общества, государства по обеспечению безопасности;

- интеграция с международными системами безопасности.

Необходимо отметить, что попытки сформировать новую парадигму государственной безопасности в первые годы становления суверенной России базировались на романтических и в некоторой степени примитивных представлениях об отсутствии реальных вызовов и угроз в современном мире. Игнорировались факты ожесточенной международной экономической конкуренции, конфликтность и противоречивость современной мировой системы, где столкновение сил и интересов не затухает, но меняет свои конфигурации. Попытки выстроить реальную политику на основе концепции баланса интересов, моделей партнерства и международного сотрудничества, принципов защиты прав человека и безопасности личности при идеализации данных положений и отсутствии необходимых ресурсов и механизмов для защиты собственных национальных интересов привели к серьезной сдаче геополитических и геоэкономических позиций страны.

В то же время возник целый ряд принципиально новых и опасных угроз, как в политической, так и в экономической сферах. Поэтому работа над формированием новой парадигмы национальной безопасности России не прекращалась.

1.2. Концепция национальной безопасности

С середины 1994 г. под эгидой созданного и набравшего необходимый государственный авторитет Совета безопасности начинается разработка концепции экономической безопасности, которая была обнародована в начале 1995 г. как Государственная стратегия экономической безопасности Российской Федерации (Основные положения) и введена в действие Указом Президента Российской Федерации от 29.04.96 г. № 608 [3].

В период 1995-1997 гг. был уточнен ряд принципиальных положений объявленной ранее парадигмы национальной безопасности. Разработанная система включает определение концепции национальной безопасности как опорной конструкции, непосредственно связанной с национальной идеей, национальными ценностями и традициями, вековыми интересами населения и государства. На базе этой концепции и сформировалась стратегия национальной безопасности, в которой отражаются фундаментальные цели, приоритеты, весь комплекс жизненно важных интересов

страны. Временные горизонты, охватываемые стратегией, простираются на период до 50 лет.

Руководствуясь концепцией и стратегией, государство и его соответствующие органы получили возможность разрабатывать долгосрочные прогнозы и программы обеспечения национальной безопасности по основным направлениям их реализации через проведение политики национальной безопасности.

Проблемы обеспечения экономической безопасности страны, стабильного экономического развития государства и общества стоят перед многими странами мира. Современное социально-экономическое положение России обусловливает чрезвычайную актуальность целенаправленной деятельности государства в сфере обеспечения экономической безопасности страны, российского общества и каждого гражданина в отдельности.

Понятие "экономическая безопасность" неразрывно связано с понятием "национальная безопасность". Термин "национальная безопасность" прочно вошел в жизнь современного мира и стал частью внутренней и внешней политики многих стран. Например, США разрабатывают доктрину, концепцию и стратегию своей национальной безопасности, где особое место уделено вопросам экономической безопасности. Поскольку экономика является одной из жизненно важных сторон деятельности личности, общества и государства, то обеспечение национальной безопасности по существу невозможно без обеспечения экономической.

Национальная безопасность - чрезвычайно сложная многоуровневая функциональная система, в которой непрерывно происходят процессы взаимодействия и противоборства жизненно важных интересов личности, общества, государства с угрозами этим интересам, как внутренними, так и внешними. При этом взаимодействии и противоборстве интересы и угрозы постоянно испытывают воздействие со стороны других элементов системы национальной безопасности: факторов внутренней и внешней окружающей среды и действий управляющей системы (рисунок 1). В качестве целевой функции этой системы выступает степень защищенности данных интересов от угроз.

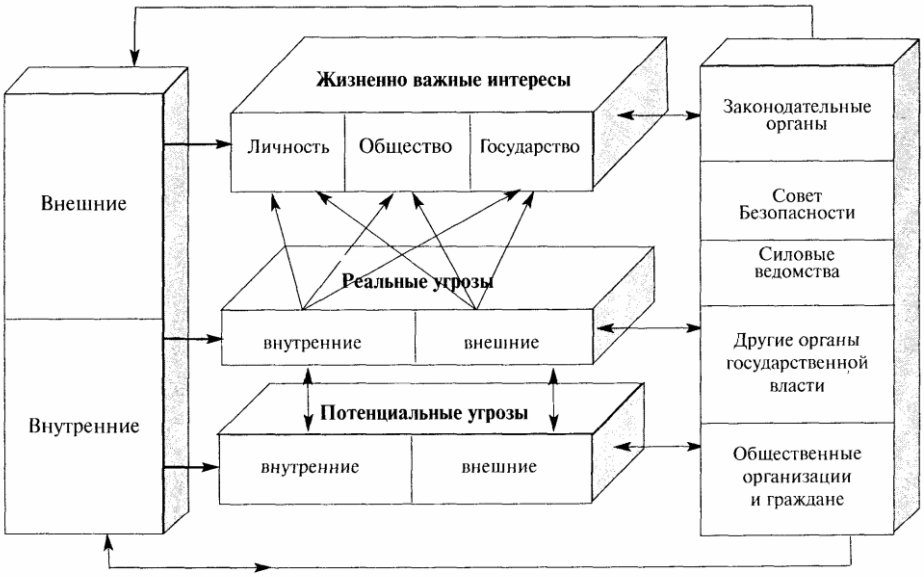


Рисунок 1. Система национальной безопасности

При этом следует различать систему национальной безопасности и систему обеспечения национальной безопасности. Первая - функциональная система, отражающая процессы взаимодействия интересов и угроз, вторая - организационная система органов, сил, средств, различных организаций, призванных решать задачи по обеспечению национальной безопасности.

Важнейшим компонентом национальной безопасности, её материальным фундаментом, выступает экономическая безопасность.

Все элементы триады “личность-общество-государство” одновременно являются и объектом безопасности, и субъектом ее обеспечения.

Рассматривая различные стороны национальной безопасности, нельзя обойти экономические аспекты.

Проблемы обеспечения экономической безопасности России, как непременного условия стабилизации ее текущего состояния и развития, привлекают к себе все более пристальное внимание ученых и общественности. Такое внимание отнюдь не случайно. Принципиально важно раскрыть суть проблемы, выявить реальные угрозы, предложить надежные и эффективные методы их парирования. Реализация национальных интересов России в большинстве случаев возможна только при условии наличия достаточных экономических возможностей и устойчивого экономического развития. Таким образом, можно говорить о том, что экономической безопасности принадлежит определяющее место в общей системе национальной безопасности.

Концепция национальной безопасности Российской Федерации исходит из перспектив многополярного мира, в котором наряду с военно-силовыми факторами возрастает роль экономических, политических, научно-технических, экологических и информационных условий.

В Концепции учитывается, что в настоящее время обостряется международная конкуренция за обладание природными, технологическими, информационными ресурсами, рынками сбыта. При этом баланс позитивных и негативных сторон нынешней фазы становления многополярного мира подвижен, что повышает уровень требований к здравому смыслу в политике и экономике.

В Концепции признано, что, хотя в целом влияние России на решение кардинальных вопросов международной жизни за годы реформирования снизилось, страна имеет все предпосылки для того, чтобы поддержать и упрочить свои позиции великой державы, занимающей особое место на евроазиатском континенте и способной обеспечить процветание своего народа, играть важную роль в мировых процессах. Об этом свидетельствует мощный ресурсный, культурный и интеллектуальный потенциал России, ее уникальное геостратегическое положение в Евразии, усиление основ демократической государственности и многоукладной экономики. Несмотря на все политические и социально-экономические потрясения последних 10 лет, Россия сохраняется как многоукладное государство, имеющее многовековую историю и культуру, четко очерченные интересы и традиции.

Концепция впервые ввела в лексикон официальных документов понятие национальных интересов, предложила их достаточно полное определение, дала комплексную систематизацию возможных и реальных угроз, определила основные контуры, институты и механизмы защиты национальной безопасности страны.

В Концепции четко сформулировано, что национальные интересы России в области экономики являются ключевыми. В связи с этим комплексное решение проблем, связанных с реализацией национальных интересов России, возможно только на основе устойчивого функционирования многоотраслевого хозяйства высокотехнологичного, способного обеспечить ведущие отрасли экономики качественным сырьем, армию - вооружением, население и социальную сферу - предметами потребления и услугами, внешнюю торговлю - конкурентоспособными товарами.

В новой редакции Концепции национальной безопасности, принятой Указом Президента Российской Федерации от 10 января 2000 г. № 24, учтены последние веяния времени, определение национальных интересов развернуто по их основным направлениям, более современно и подробно прописаны угрозы и механизмы защиты национальной безопасности.

В частности отмечается, что в сфере экономики угрозы носят комплексный характер и обусловлены существенным сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и предметов потребления, включая предметы первой необходимости и медикаменты.

Ослабление научно-технического и технологического потенциалов страны, сокращение исследований на стратегически важных направлениях научно-технического развития, отток за рубеж специалистов, ученых и интеллектуальной собственности угрожают России утратой передовых позиций в мире, деградацией наукоемких производств, усилением внешней технологической зависимости и подрывом обороноспособности.

Негативные процессы в экономике в значительной степени лежат в основе сепаратистских устремлений ряда субъектов Российской Федерации, что ведет к усилению политической нестабильности, нарушению единого экономического пространства и ослаблению его важнейших составляющих - производственно-технологических и транспортных связей, финансово-банковской, кредитной и налоговой систем.

Экономическая дезинтеграция, социальная дифференциация общества, девальвация духовных ценностей способствует усилению напряженности во взаимоотношениях регионов и федерального центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу Российской Федерации.

Особую остроту приобретает угроза криминализации общественных отношений. Росту преступности и коррупции способствуют серьезные просчеты, допущенные на начальном этапе проведения реформ в экономической, военной, правоохранительной и иных областях государственной деятельности. Последствия этих просчетов проявляются в ослаблении правового контроля за ситуацией в стране, в сращивании отдельных элементов исполнительной и законодательной ветвей власти с криминальными структурами, проникновении последних в сферу управления банковским бизнесом, крупными производствами, торговыми организациями и товаропроводящими сетями.

Угрозу национальной безопасности создают и глубокое расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, увеличение удельного веса населения, живущего за чертой бедности, рост безработицы.

Основными задачами в области обеспечения национальной безопасности Российской Федерации в настоящее время признаны:

- своевременное прогнозирование и выявление внешних и внутренних угроз национальной безопасности;

- реализация оперативных и долгосрочных мер по предупреждению нейтрализации внутренних и внешних угроз;

- обеспечение суверенитета и территориальной целостности страны, безопасности ее приграничного пространства;

- подъем экономики и уровня жизни населения, проведение независимого и социально ориентированного экономического курса;

- преодоление научно-технической и технологической зависимости страны от внешних источников;

- обеспечение на всей территории государства личной безопасности человека и гражданина, соблюдение его конституционных прав и свобод;

- совершенствование системы государственной власти, федеративного и местного самоуправления, законодательства всех уровней; формирование гармоничных межнациональных отношений; укрепление правопорядка; сохранение социально-политической стабильности общества;

- неукоснительное соблюдение законодательства всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями;

- равноправное и взаимовыгодное сотрудничество со всеми государствами мира;

- подъем и поддержание на достаточно высоком уровне оборонного потенциала государства.

Важнейшими задачами во внешнеэкономической деятельности являются:

- создание благоприятных условий для международной интеграции российской экономики;

- расширение рынков сбыта российской продукции;

В условиях либерализации внешней торговли и обострения конкуренции на мировом рынке товаров и услуг необходимо усилить защиту интересов от отечественных товаропроизводителей. Важнейшее значение приобретает проведение сбалансированной кредитно-финансовой политики, нацеленной на поэтапное сокращение зависимости страны от внешних кредитных заимствований и укрепление ее позиций в международных финансово-экономических организациях. В целях усиления роли государства в регулировании деятельности иностранных банковских, страховых и инвестиционных компаний следует ввести определенные и обоснованные

ограничения на передачу в эксплуатацию зарубежным компаниям месторождений стратегических природных ресурсов, телекоммуникаций, транспортных и товаропроводящих сетей. Эффективные меры должны быть приняты также в сфере валютного регулирования и контроля в целях создания условий для прекращения расчетов в иностранной валюте на внутреннем рынке и предотвращения бесконтрольного вывоза капитала.

Основными направлениями обеспечения национальной безопасности Российской Федерации во внутриэкономической деятельности следует считать:

- правовую поддержку реформ и создание эффективного механизма контроля за соблюдением законодательства страны;

- усиление государственного регулирования в экономике;

- принятие необходимых мер по преодолению последствий экономического кризиса, сохранение и развитие научно-технического, технологического и производственного потенциалов, переход к экономическому росту при снижении вероятности техногенных катастроф, повышение конкурентоспособности отечественной промышленной продукции, подъем благосостояния населения.

Переход к высокоэффективной и социально ориентированной рыночной экономике должен осуществляться путем постепенного формирования оптимальных механизмов организации производства и распределения товаров и услуг в целях максимально возможного роста благосостояния общества и каждого гражданина.

На первый план выдвигаются задачи, связанные с устранением деформаций в структуре российской экономики, с обеспечением опережающего роста производства наукоемкой продукции и продукции высокой степени переработки, с поддержкой отраслей, составляющих основу расширенного воспроизводства, обеспечением полной занятости населения.

Существенное значение имеют усиление государственной поддержки инвестиционной и инновационной активности; принятие мер по созданию устойчивой банковской системы, отвечающей интересам реальной экономики; облегчение доступа предприятий к долгосрочным кредитам на финансирование капитальных вложений, реальная помощь государства, реализация целевых программ структурной перестройки промышленности. Как никогда ранее, самыми приоритетными становятся задачи по опережающему развитию конкурентоспособных отраслей и производств, расширению рынка наукоемкой продукции. В целях их решения должны быть приняты меры, стимулирующие передачу новых военных технологий в гражданское производство, введен механизм выявления и развития прогрессивных технологий, повышающих конкурентоспособность российских предприятий на мировом рынке.

Важное значение имеет концентрация финансовых и материальных ресурсов на приоритетных направлениях науки и техники, оказание поддержки ведущим научным школам, ускоренное формирование научно-технического задела и национальной технологической базы, привлечение для этих целей частного капитала, в том числе путем организации фондов и использования грантов, реализация программ первоочередного развития территорий, обладающих высоким научно-техническим потенциалом, защита государством интеллектуальной собственности внутри страны и за рубежом, расширение общедоступной сети научно-технической и коммерческой

информации, создание равных условий для роста и повышения конкурентоспособности предприятий независимости от формы собственности, в том числе поощрение частного предпринимательства во всех сферах, где это способствует росту общественного благосостояния, прогрессу науки и образования, духовному и нравственному развитию членов общества, защите прав потребителя.

Таким образом, обеспечение экономической безопасности является принципиально важным в целях укрепления государства, реального обеспечения социальных гарантий, развития механизмов коллективной ответственности и демократического, социального партнерства.

Структура экономической безопасности по существу представлена в предложенной развернутой формулировке и состоит, по нашему мнению, из трех частей.

Первая – это достаточность финансово-экономических ресурсов для обеспечения требуемого уровня национальной безопасности страны, в первую очередь, ее обороноспособности за счет совершенствования и развития вооруженных сил. Эта составляющая присуща для всех наиболее развитых стран мира и по существу не вызывает ни у кого сомнения. Обеспечивается она государством исключительно за счет бюджетных средств.

Вторая – создание наиболее благоприятных условий для стабильного развития экономики в стране, причем для всех легальных секторов экономики. Эти условия должны распространяться на государственный и частный сектора, в том числе на частное предпринимательство, т.е. на все уровни - государства, общества и личности. Создание этих условий будет одновременно способствовать росту наполняемости бюджета, т.е. обеспечению первой составляющей.

Третья – защита экономических интересов государства, общества и личности от внешних и внутренних угроз. Эта составляющая необходима для всех стран, охваченных глобальной экономикой. В глобальной экономике в условиях международной кооперации любые изменения, тем более катастрофические, в той или иной мере отражаются на всех ее участниках и поэтому требуются эффективные адекватные меры в случаях возникновения таких ситуаций.

Все три составляющие тесно взаимосвязаны, примерно равнозначны и поэтому приведены в одном определении.

Принципиально важным является баланс (гармоничное сочетание) национальной и экономической безопасности. Дело в том, что с экономической точки зрения обеспечение национальной безопасности в основной своей части – обороноспособности, это по существу расходная (затратная) часть, необходимость которой определяется гипотетически -уровнем предотвращенного ущерба в случае войны, однако одновременно для баланса должна быть и доходная часть, обеспечиваемая созданием наиболее благоприятных условий для жизнедеятельности субъектов хозяйствования (физических и юридических лиц) в экономической сфере и защищенностью их интересов.

Концепция национальной безопасности Российской Федерации исходит из перспектив многополярного мира, в котором наряду с военно-силовыми факторами возрастает роль экономических, политических, научно-технических, экологических и информационных условий.

В Концепции учитывается, что в настоящее время обостряется международная конкуренция за обладание природными, технологическими, информационными ресурсами, рынками сбыта. При этом баланс позитивных и негативных сторон нынешней фазы становления многополярного мира подвижен, что повышает уровень требований к здравому смыслу в политике и экономике .

В Концепции признано, что, хотя в целом влияние России на решение кардинальных вопросов международной жизни за годы реформирования снизилось, страна имеет все предпосылки для того, чтобы поддержать и упрочить свои позиции великой державы, занимающей особое место на евроазиатском континенте и способной обеспечить процветание своего народа, играть важную роль в мировых процессах. Об этом свидетельствует мощный ресурсный, культурный и интеллектуальный потенциал России, ее уникальное геостратегическое положение в Евразии, усиление основ демократической государственнос¬ти и многоукладной экономики. Несмотря на все политические и социально-экономические потрясения последних 10 лет, Россия сохраняется как многоукладное государство, имеющее многовековую историю и культуру, четко очерченные интересы и традиции.

Концепция впервые ввела в лексикон официальных документов понятие национальных интересов, предложила их достаточно полное определение, дала комплексную систематизацию возможных и реальных угроз, определила основные контуры, институты и механизмы защиты национальной безопасности страны.

В Концепции четко сформулировано, что национальные интересы России в области экономики являются ключевыми. В связи с этим комплексное решение проблем, связанных с реализацией национальных интересов России, возможно только на основе устойчивого функционирования многоотраслевого хозяйства высокотехнологичного, способного обеспечить ведущие отрасли экономики качественным сырьем, армию - вооружением, население и социальную сферу - предметами потребления и услугами, внешнюю торговлю - конкурентоспособными товарами.

В новой редакции Концепции национальной безопасности, принятой Ука¬зом Президента Российской Федерации от 10 января 2000 г. № 24, учтены последние веяния времени, определение национальных интересов развернуто по их основным направлениям, более современно и подробно прописаны угрозы и механизмы защиты национальной безопасности.

В частности отмечается, что в сфере экономики угрозы носят комплексный характер и обусловлены существенным сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и предметов потребления, включая предметы первой необходимости и медикаменты.

Ослабление научно-технического и технологического потенциалов страны, сокращение исследований на стратегически важных направлениях научно-технического развития, отток за рубеж специалистов, ученых и интеллектуальной собственности угрожают России утратой передовых позиций в мире, деградацией наукоемких производств, усилением внешней технологической зависимости и

подрывом обороноспособности.

Негативные процессы в экономике в значительной степени лежат в основе сепаратистских устремлений ряда субъектов Российской Федерации, что ведет к усилению политической нестабильности, нарушению единого экономического пространства и ослаблению его важнейших составляющих - производственно-технологических и транспортных связей, финансово-банковской, кредитной и налоговой систем.

Экономическая дезинтеграция, социальная дифференциация общества, девальвация духовных ценностей способствует усилению напряженности во взаимоотношениях регионов и федерального центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу Российской Федерации.

Особую остроту приобретает угроза криминализации общественных отношений. Росту преступности и коррупции способствуют серьезные просчеты, допущенные на начальном этапе проведения реформ в экономической, военной, правоохранительной и иных областях государственной деятельности. Последствия этих просчетов проявляются в ослаблении правового контроля за ситуацией в стране, в сращивании отдельных элементов исполнительной и законодательной ветвей власти с криминальными структурами, проникновении последних в сферу управления банковским бизнесом, крупными производствами, торговыми организациями и товаропроводящими сетями.

Угрозу национальной безопасности создают и глубокое расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, увеличение удельного веса населения, живущего за чертой бедности, рост безработицы .

Основными задачами в области обеспечения национальной безопасности Российской Федерации в настоящее время признаны:

- своевременное прогнозирование и выявление внешних и внутренних угроз национальной безопасности;

- реализация оперативных и долгосрочных мер по предупреждению нейтрализации внутренних и внешних угроз;

- обеспечение суверенитета и территориальной целостности страны, безопасности ее приграничного пространства;

- подъем экономики и уровня жизни населения, проведение независимого и социально ориентированного экономического курса;

- преодоление научно-технической и технологической зависимости страны от внешних источников;

- обеспечение на всей территории государства личной безопасности человека и гражданина, соблюдение его конституционных прав и свобод;

- совершенствование системы государственной власти, федеративного и местного самоуправления, законодательства всех уровней; формирование гармоничных межнациональных отношений; укрепление правопорядка; сохранение социально-политической стабильности общества;

- неукоснительное соблюдение законодательства всеми гражданами, должностными лицами, государственными органами, политическими партиями, общественными и религиозными организациями;

- равноправное и взаимовыгодное сотрудничество со всеми государствами;

- подъем и поддержание на достаточно высоком уровне оборонного потенциала государства.

Важнейшими задачами во внешнеэкономической деятельности являются:

- создание благоприятных условий для международной интеграции российской экономики;

- расширение рынков сбыта российской продукции.

В условиях либерализации внешней торговли и обострения конкуренции на мировом рынке товаров и услуг необходимо усилить защиту интересов от отечественных товаропроизводителей. Важнейшее значение приобретает проведение сбалансированной кредитно-финансовой политики, нацеленной на поэтапное сокращение зависимости страны от внешних кредитных заимствований и укрепление ее позиций в международных финансово-экономических организациях. В целях усиления роли государства в регулировании деятельности иностранных банковских, страховых и инвестиционных компаний следует ввести определенные и обоснованные ограничения на передачу в эксплуатацию зарубежным компаниям месторождений стратегических природных ресурсов, телекоммуникаций, транспортных и товаропроводящих сетей. Эффективные меры должны быть приняты также в сфере валютного регулирования и контроля в целях создания условий для прекращения расчетов в иностранной валюте на внутреннем рынке и предотвращения бесконтрольного вывоза капитала.

Основными направлениями обеспечения национальной безопасности Российской Федерации во внутриэкономической деятельности следует считать:

- правовую поддержку реформ и создание эффективного механизма контроля за соблюдением законодательства страны;

- усиление государственного регулирования в экономике;
- принятие необходимых мер по преодолению последствий экономического кризиса, сохранение и развитие научно-технического, технологического и производственного потенциалов, переход к экономическому росту при снижении вероятности техногенных катастроф, повышение конкурентоспособности отечественной промышленной продукции, подъем благосостояния населения.

Переход к высокоэффективной и социально ориентированной рыночной экономике должен осуществляться путем постепенного формирования оптимальных механизмов организации производства и распределения товаров и услуг в целях максимально возможного роста благосостояния общества и каждого гражданина.

На первый план выдвигаются задачи, связанные с устранением деформаций в структуре российской экономики, с обеспечением опережающего роста производства наукоемкой продукции и продукции высокой степени переработки, с поддержкой отраслей, составляющих основу расширенного воспроизводства, обеспечением

полной занятости населения.

Существенное значение имеют усиление государственной поддержки инвестиционной и инновационной активности; принятие мер по созданию устойчивой банковской системы, отвечающей интересам реальной экономики; облегчение доступа предприятий к долгосрочным кредитам на финансирование капитальных вложений, реальная помощь государства, реализация целевых программ структурной перестройки промышленности.

Как никогда ранее, самыми приоритетными становятся задачи по опережающему развитию конкурентоспособных отраслей и производств, расширению рынка наукоемкой продукции. В целях их решения должны быть приняты меры, стимулирующие передачу новых военных технологий в гражданское производство, введен механизм выявления и развития прогрессивных технологий, повышающих конкурентоспособность российских предприятий на мировом рынке.

Важное значение имеет концентрация финансовых и материальных ресурсов на приоритетных направлениях науки и техники, оказание поддержки ведущим научным школам, ускоренное формирование научно-технического задела и национальной технологической базы, привлечение для этих целей частного капитала, в том числе путем организации фондов и использования грантов, реализация программ первоочередного развития территорий, обладающих высоким научно-техническим потенциалом, защита государством интеллектуальной собственности внутри страны и за рубежом, расширение общедоступной сети научно-технической и коммерческой информации, создание равных условий для роста и повышения конкурентоспособности предприятий независимости от формы собственности, в том числе поощрение частного предпринимательства во всех сферах, где это способствует росту общественного благосостояния, прогрессу науки и образования, духовному и нравственному развитию членов общества, защите прав потребителя.

Таким образом, обеспечение экономической безопасности является принципиально важным в целях укрепления государства, реального обеспечения социальных гарантий, развития механизмов коллективной ответственности и демократического, социального партнерства.

1.3. Критерии и показатели экономической безопасности национальной экономики

Существует тесная взаимосвязь экономической безопасности с системой национально-государственных интересов. Именно через категорию национально-государственных интересов сплетаются воедино проблемы экономического потенциала и экономической мощи государства: состояние генофонда нации, предпосылки и условия ее физического здоровья и социально-культурного процветания; геополитические и геоэкономические позиции страны в современном мире.

На первых этапах российских экономических реформ вопрос об их соответствии национально-государственным интересам России, к сожалению, не ставился. Рыночные реформы сами по себе считались приоритетом номер один, проблемы

вариантов их проведения игнорировались.

Национально-государственные интересы можно определить как круг жизненно важных интересов всех этнических и социальных групп общества, которые:

а) в цивилизационно-культурном смысле исторически самоопределяются в качестве единой нации;

б) в политическом плане исторически само организуются как государство.

Экономическая безопасность означает надежную, обеспеченную всеми необходимыми средствами и институтами государства (включая силовые структуры и спецслужбы) защищенность национально-государственных интересов в сфере экономики от внутренних и внешних угроз, экономических ущербов.

Состояние экономической безопасности оценивается перечнем параметров, критериев и индикаторов, определяющих пороговые значения функционирования экономической системы. Как свидетельствует опыт многих зарубежных стран, за пределами этих значений система теряет способность к динамичному саморазвитию и конкурентоспособность на внутреннем и внешнем рынках, становится объектом экспансии инонациональных и транснациональных монополий, в ней усиливается коррупция и криминалитет.

Виды экономической безопасности определяются в зависимости от сфер и отраслей экономической деятельности и соответствующих рынков. В реальном секторе экономики речь идет в первую очередь о производственно-технологической, промышленной безопасности. Однако этими сферами не исчерпывается вся проблематика этого вида. Одновременно необходимо рассматривать, в чьих интересах происходит распределение и перераспределение национального богатства страны, проводится приватизация государственной собственности, деиндустриализация экономики; как используются экспортный потенциал и рынки внутри страны под напором дешевого импорта.

Энергетические проблемы современной экономики требуют выделения в самостоятельный вид энергетической безопасности. Это связано как с ограниченностью и дороговизной источников энергии, так и с конкурентной борьбой за контроль над этими ресурсами между предприятиями-производителями энергоносителей и энергопроводящими сетями. Сегодня энергетическая политика во всех регионах мира глобализуется и превращается в один из главных объектов геополитического и геоэкономического планирования.

Инфляционная безопасность выражается в росте цен. Но она, как правило, связана с общей сбалансированностью финансовых потоков и равновесием в экономике. Рост цен может отражать конъюнктуру на финансовых рынках, рынках валюты, состояние бюджетного, торгового и платежного балансов страны. Поэтому общий инфляционный потенциал экономики, складывающийся в результате всей совокупности факторов, часто говорит о финансовой безопасности вообще, частными проявлениями которой и являются инфляционная, валютная и другие подвиды, связанные с бюджетом, банками, рынками ценных бумаг.

Самостоятельный вид образует внешнеэкономическая безопасность, обусловленная взаимодействием национальной и мировой экономик, внутренних и внешних рынков.

Она проявляется в конкурентоспособности отечественных экспортеров, внутренних производителей, экономики в целом, отражается в показателях внешней торговли в структуре ВВП; в результатах годовых платежных и торговых балансов; в динамике и структуре внешнеторгового оборота.

Возрастающую роль в современной экономике играет интеллектуальная безопасность. Обеспечение безопасности в этой области должно достигаться с помощью патентной защиты, таможенного регулирования.

Еще один вид экономической безопасности - информационная безопасность, особая роль информации и информационных технологий в организации современных рынков, бизнеса.

Мир пока продолжает жить по законам баланса сил, а не согласования интересов. В настоящее время колоссальную роль играют вызовы, идущие от глобализации мировой экономики. Глобализация - процесс объективный., о нем сейчас говорится много, и он оценивается неоднозначно. Без сомнения, надо развести понятия объективной глобализации и той парадигмы, по которой она сегодня вполне регулируемо развивается под патронажем США и их геополитических партнеров. Процесс глобализации идет в русле неолиберальной парадигмы, он носит целенаправленный характер и отражает интересы ключевых субъектов глобальной экономики. Это моноцентричная глобализация, которая в интересах ведущих западных держав и транснациональных капиталов стремится ликвидировать национальные и даже региональные (геополитические) границы.

Однако надо иметь в виду, что экономическое развитие не терпит монопольного доминирования. И объективно полицентричная модель глобализации в большей степени соответствует как реалиям мировой экономики, так и интересам государств и регионов, не входящих в «золотой миллиард».

России важно выработать собственное видение своего места в глобализации, выстроить соответствующие геостратегические концепции глобализации. Без концепции и активной внешнеэкономической и политической работы страна непременно выдвинется на периферию современного мирового экономического пространства.

Отдельного рассмотрения требует вопрос о субъектной структуре глобальной экономики. Для этого необходимо проанализировать:

✓ процесс объединения национальных государств в интеграционные союзы;

✓ транснациональные капиталы, транснациональные корпорации (ТНК) и банки как их организационно-правовые формы;

✓ международные экономические институты регулирования и координации.

Экономически развитые государства и их различные интеграционные образования активно содействуют деятельности транснациональных корпораций, происхождение или базирование которых так или иначе связано с соответствующими национальными интересами экономического, дипломатического, а часто и военно-политического характера. Эти государства, будучи наиболее влиятельными членами МВФ, ВТО, МБ и других международных экономических институтов, оказывают решающее

воздействие на их деятельность. Международные экономические институты в свою очередь, с одной стороны, демонстрируют финансово-экономическую многостороннюю поддержку политики западных держав и прежде всего США; с другой стороны, активно формируют институциональные основы нового экономического миропорядка, в котором доминируют транснациональные капиталы и международные финансовые рынки.

Вопрос о том, на какой платформе возможно развитие глобализации и как сочетать современный глобализм с идеями многополюсного мира, интересами национальных государств, отдельных регионов, остается открытым.

В условиях образования новых метасубъектов мировой экономики и геополитики новых центров силы, их иерархий и балансов складываются совершенно особые, ранее не проявлявшиеся реалии функционирования национальных государств. Государство становится сильным и ответственным субъектом сохранения национальных интересов страны перед лицом современных региональных союзов и интеграции, ТНК, наднациональных органов международного планирования, регулирования, координации. От понимания этого зависит его место в новых мировых иерархиях, способность защиты политического и экономического суверенитета, его воздействие на международные и внутриполитические процессы. Для России это вдвойне актуально в силу ее совершенно особого геополитического и геостратегического положения, своеобразия исторического периода, переживаемого страной.

Национально-государственные интересы ведущих стран мира, конкурентные позиции национальных экономик или их интеграционных союзов, корпоративные интересы транснациональных компаний продолжают оставаться важнейшими приоритетами и мотивами действий в международных отношениях.

Добровольный отказ России от преимуществ и выгод положения второй сверхдержавы мира, одностороннее уклонение от мирового соперничества в геополитических и геоэкономических системах координат в первые годы реформирования не столько обеспечило «возвращение в мировое сообщество», сколько понизило статус страны до уровня региональной державы в мировом сообществе. Утверждение России в качестве полноправного члена мирового сообщества, формирование свободных от конфронтации отношений с ведущими странами Запада, ее вхождение в международные экономические организации должны происходить без какого-либо ущемления ее национально-государственных интересов, параллельно с восстановлением ее статуса мировой экономической державы. Все, что противодействует данной стратегии, чревато угрозами и ущербами для экономической безопасности страны. Политика реформ также должна находиться в русле данной стратегии.

Содержание экономической безопасности раскрывается через ее ключевые понятия, связанные категориями угроз и параметров, критериев и индикаторов экономической безопасности.

Методологический ключ к классификации угроз экономической безопасности содержится в Государственной стратегии экономической безопасности (Основные положения) [4].

1. Увеличение имущественной дифференциации населения подрывает социальный мир и общественное согласие. Относительный баланс социальных интересов может быть нарушен в результате:

- расслоения общества на узкий круг богатых и преобладающую массу бедных, не уверенных в своем будущем людей;

- увеличения доли бедных слоев населения в городе по сравнению с деревней, что создает социальную и криминальную напряженность и почву для широкого распространения относительно новых для России негативных явлений - наркомании, организованной преступности, проституции и т. д.;

- роста числа безработных, что может привести к социальным конфликтам;
- задержки выплаты заработной платы, пенсий, пособий, остановки предприятий и т. д.

2. Деформированность структуры российской экономики обусловлена такими факторами, как:

- усиление топливно-сырьевой направленности экономики;

- отставание разведки запасов полезных ископаемых от их добычи;

- низкая конкурентоспособность продукции большинства отечественных предприятий;

- свертывание производства в жизненно важных отраслях обрабатывающей промышленности, прежде всего в машиностроении;

- снижение результативности, расширение технологического единства научных исследований и разработок, распад сложившихся научных коллективов и на этой основе подрыв научно-технического потенциала России;

- завоевание иностранными фирмами внутреннего рынка России по многим видам товаров народного потребления и медикаментов;

- приобретение иностранными фирмами российских предприятий в целях вытеснения отечественной продукции как с внешнего, так и с внутреннего рынков;

- рост внешнего долга России и связанное с этим увеличение расходов бюджета на его погашение.

3. Угрозу неравномерности социально-экономического развития регионов обусловливают такие важнейшие факторы, как:

- объективно существующие различия в уровне социально-экономического развития регионов, наличие депрессивных, кризисных и отсталых в социально-экономическом отношении районов на фоне структурных сдвигов в промышленном производстве, сопровождающихся резким уменьшением доли обрабатывающих производств;

- нарушение производственно-технологических связей между предприятиями отдельных регионов России;

- увеличение разрыва в уровне производства национального дохода на душу населения между отдельными субъектами Российской Федерации.

4. Причинами криминализации общества и хозяйственной деятельности стали:

- рост безработицы, поскольку значительная часть преступлений совершается лицами, не имеющими постоянного источника дохода;

- сращивание части чиновничества государственных органов с организованной преступностью, возможность доступа криминальных структур к управлению определенной долей производства и их проникновение в различные властные образования;

- ослабление системы государственного контроля, что всегда приводит к расширению деятельности криминальных структур на внутреннем финансовом рынке, в сфере приватизации, экспортно-импортных операций и торговли.

Предотвращение или смягчение последствий действия угроз экономической безопасности требует четкого определения и постоянного мониторинга факторов, подрывающих устойчивость социально-экономической системы государства.

В теоретическом плане проблема параметров, критериев и индикаторов (показателей) экономической безопасности во многом связана с результатами функционирования экономики в целом. Соответственно на первый план выдвигаются макроэкономические показатели.

Параметрами макроэкономической деятельности принято называть те переменные, которые характеризуют тот или иной вариант макроэкономической политики государства (политика регулирования спроса либо предложения; в рамках политики регулирования спроса - кредитно-денежная политика валютного курса, бюджетно-налоговая, таможенная политика).

В области кредитно-денежной политики — это количество денег в обращении, реальные деньги (денежная масса, соотнесенная с ростом цен), динамика денежной массы, скорость денег в обращении, процентные ставки.

В области бюджетно-налоговой политики - это налоговые ставки, количество налогов, правительственные расходы, правительственные субсидии, величина бюджетного дефицита. Эти параметры могут быть весьма жесткими в критические периоды экономического развития. Жесткость кредитно-денежной политики связана с ограничением денежного предложения, бюджетно-налоговой - с ограничением правительственных расходов, уровнем налогообложения.

Обычно различные виды макроэкономической политики альтернативны по степени жесткости: к примеру, мягкая кредитно-денежная и жесткая бюджетно-налоговая, или наоборот. Удвоенная жесткость политики приводит к тому, что экономика испытывает двойной шок, и в рамках регулирования спроса трудно уравновесить его последствия.

К сожалению, такое положение сложилось на старте рыночных реформ в России. Сверхжесткая политика денежного предложения, с последствиями которой страна не может справиться до сих пор, проводилась параллельно со сверхжесткой бюджетно-налоговой политикой, в ходе которой беспрецедентный взлет налогового бремени сочетался с единовременным сбросом правительственных расходов. Игнорирование в процессе подбора параметров макроэкономической политики соображений экономической безопасности и привело к тому, что за 10 лет реформ страна не

преодолела последствия системного кризиса.

Наиболее эффективно результаты функционирования экономики оцениваются тремя общими экономическими критериями: инфляцией, экономическим ростом (спадом), безработицей. На базе этих критериев рассчитываются показатели темпов инфляции, экономического роста (спада), уровня безработицы. Это исходные параметры, на основе которых с различной степенью детализации и учета разнообразных факторов макроэкономической динамики можно развернуть достаточно представительную систему показателей.

Целесообразно использовать и такие индикаторы, как процентные ставки, данные важнейших балансов (госбюджета, торгового, платежного), величина внутреннего госдолга, внешняя задолженность.

Следует подчеркнуть, что игнорирование стандартных зависимостей параметров экономической политики, пороговых критериев безопасности, показателей экономической динамики в конечном счете и привело к событиям августа 1998 г., когда страна оказалась фактически в состоянии финансового дефолта.

На основе перечисленных критериев формируется примерный перечень параметров пороговых значений экономической безопасности, по которым можно отслеживать ее состояние и динамику, оказывать управляющее воздействие. В этот перечень целесообразно включить показатели, которые в наибольшей степени отражают агрегированные позиции:

- динамику и структуру валового внутреннего продукта, объемы и темпы промышленного производства, отраслевую и региональную структуру хозяйства и динамику отдельных отраслей, капитальные вложения и т. д.;

- состояние природно-ресурсного, производственного и научно-технического потенциалов страны;

- способность хозяйственного механизма адаптироваться к меняющимся внутренним и внешним факторам (темпы инфляции, дефицит государственного бюджета, воздействие внешнеэкономических факторов, стабильность национальной валюты, внутренняя и внешняя задолженность и т. п.);

- степень развития финансово-бюджетной и кредитной систем;

- качество жизни населения (валовой внутренний продукт на душу населения), уровень безработицы и дифференциации доходов, обеспеченность основных групп населения материальными благами и услугами, состояние окружающей среды и т. п.

Таким образом, существует целый ряд количественных и качественных индикаторов, позволяющих объективно и комплексно оценить уровень обеспечения экономической безопасности не только страны в целом, но и каждого региона.

1.4. Оценка бизнеса на наличие угроз безопасности

Необходимо отметить, что среди возможных проблем чаще всего, отмечаются случаи

неправомерного использования материальных (финансовых) ресурсов предприятия. Но, кроме того, существует угроза непосредственного подчинения предпринимателя (или его фирмы) сторонним организациям и тем самым получения экономических выгод от его деятельности.

Рейтинг обращений отечественных бизнесменов за помощью в охранные фирмы выглядит следующим образом (по убывающей):

1) Проблема возврата средств (не поступает плата за отгруженный товар, не поступает оплаченный товар, не возвращается в указанный срок кредит);

2) Проблема личной безопасности бизнесменов и членов их семей в связи с угрозами и вымогательством;

3) Хищение грузов на транспорте;

4) Кражи личного имущества в квартирах, офисах, коттеджах, загородных строениях; ограбления; угоны автомобилей;

5) Похищение коммерческой информации (кража документов, их копирование, съем информации с компьютеров и факсов, прослушивание и запись телефонных сообщений, разговоров в помещениях, подкуп сотрудников);

6) Кражи и ограбления в магазинах, складских и производственных помещениях;

7) Порча имущества и товаров. Поджоги.

Итак, вы посмотрели статистику обращений отечественных предприятий в охранные фирмы. Теперь попробуем понять, как определить, для кого и какой интерес будет представлять деятельность вашей фирмы.

В настоящее время в России, деятельностью любого хозяйствующего субъекта в основном интересуются:

- государство;
- конкуренты;
- криминальные структуры;
- его собственный персонал.

Государство в основном контролирует правовую основу вашей деятельности – зарегистрировано ли предприятие, есть ли лицензии, соответствующие вашему виду деятельности и исправно ли вы платите налоги. Кроме того, у правоохранительных органов интерес могут вызвать любые ваши действия нарушающие действующее законодательство. Поэтому, для того чтобы определить степень интереса государства к вам, посмотрите, какие ваши действия могут быть расценены различными контролирующими государственными органами как сомнительные или противоправные. Например, налоговой инспекцией.

У остальных «интересующихся» интерес носит, как правило, сугубо материальный характер.

Интерес криминальных структур. Необходимо отдавать себе отчет в том, что если ваше

предприятие в силу специфики своей деятельности попадает в зону повышенного интереса криминальных структур, то избежать общения с ними вам вряд ли удастся. Так что в этом случае лучше заранее оценить свои силы. Круг этих интересов на данной территории, если вы сами их не очень хорошо представляете, вам помогут определить специалисты (например, сотрудники детективных агентств или информационно-аналитических служб).

Кроме того, необходимо помнить, что вы рискуете привлечь к себе повышенное внимание преступных группировок, применяя методы, нарушающие требования законодательства или деловой этики.

Но, даже если вы будете вести бизнес по всем правилам, все равно есть риск встретиться с криминальным давлением.

Такое давление может возникнуть не только в случае проявления непосредственного интереса к вашей деятельности со стороны криминальных структур, но и как форма **недобросовестной конкуренции**.

Дело в том, что часто недобросовестная конкуренция не только осуществляется незаконными методами, но и при этом, в качестве средств воздействия используются криминальные структуры.

Кроме того, предприятие, а вернее его финансовые средства, представляют большой интерес и для разного рода мошенников, деятельность которых так же можно отнести к криминальной.

Основными способами для достижения цели у мошенников являются обман, введение в заблуждение, злоупотребление доверием.

Один из видов мошенничества – использование фальшивых документов (подделка печатей и штампов) реальных или вымышленных фирм. Данный способ основан на индивидуальных способностях мошенника, использующего доверие сотрудников, внушаемость, некомпетентность, халатность.

Встречаются и более изощренные способы мошенничества. Например, фирмы, созданные только для того, чтобы, набрав заказы, получить деньги по предоплате и исчезнуть. Здесь встречаются и довольно хитроумные комбинации.

Одна из фирм, занимающаяся перепродажей товара из-за рубежа, для того чтобы привлечь клиентов снизила отпускные цены на товары ниже закупочных. От клиентов не было отбоя. Договоры поначалу точно выполнялись, имидж компании сомнений не вызывал, число клиентов росло. Создалась обычная пирамида. Естественно, вскоре руководство фирмы исчезло с деньгами, перечисленными по предоплате.

Изощренные мошенники часто проходят процедуру регистрации вполне легально и некоторое время добросовестно работают. При этом ни учредители, ни непосредственные руководители могут и не быть замеченными в каких-либо махинациях ранее. Выявить таких можно только с помощью системы достаточно сложных проверок руководителей, учредителей, их связей и анализа деятельности. Это под силу только специализированной фирме.

Но обычно, для выявления возможного мошенничества достаточно получить информацию об организации, ее деятельности (прошлой и настоящей) и учредителях.

Поэтому, всегда нужно четко знать, где и какую информацию вы можете получить.

Выбор способа получения информации зависит от вас. Но нецелесообразно использовать какой-то один: рациональное решение лежит в области их комбинирования в зависимости от ситуации.

Конкуренты всегда проявляют интерес к вашей деятельности, даже если вы об этом и не догадываетесь. Вопрос лишь в том – что является предметом столь пристального внимания, и какие методы используются для его удовлетворения.

Наиболее вероятно, что интерес вызовут используемые вами новые технологии, методы работы, программы расширения и НИОКР и т.д.

Другое направление проявления повышенного интереса – это информация по настоящим и предполагаемым партнерам, клиентам, перехват выгодных контрактов и инвестиционных проектов, поставщиков и каналов сбыта

Но не стоит забывать и о недобросовестной конкуренции. Основной принцип которой заключается в стремлении любыми, даже незаконными средствами, укрепить свое положение за счет ослабления позиций конкурентов, либо за счет обмана потребителей, или путем сочетания того и другого.

Персонал, как правило, интересует стабильность в деятельности вашей организации, так как от этого зависит и стабильность заработной платы. Но бывают и исключения – это те, кто о размере своего дохода заботится сам, но... за ваш счет. Основные способы при этом – мошенничество либо воровство.

Внутреннее мошенничество.

К таковому относятся любые действия самих сотрудников, либо совершенные при их пособничестве и направленные на использование активов предприятия в личных целях. Формы его бывают различными: это и хищение, и растрата, и присвоение, и приобретение права на чужое имущество.

В соответствии с американской статистикой, в среднем каждая организация в США теряет от мошенничества более $9 в день на каждого работника и приблизительно 6% годового дохода от мошенничеств всех своих, нечистых на руку сотрудников.

Однако стоимость мошенничества и злоупотреблений в целом трудно поддается количественному измерению. Причин тому несколько:

- ✓ не все мошенничества и злоупотребления раскрываются;
- ✓ не все раскрытые факты предаются огласке;
- ✓ о некоторых случаях мошенничества собрана неполная информация;
- ✓ гражданское или уголовное преследование часто не возбуждается.

Каким бывает внутреннее мошенничество?

Выделяют три категории внутреннего мошенничества, характеризуемые такими образующими признаками, как незаконное присвоение активов, коррупция и

мошеннические утверждения.

Незаконное присвоение активов является основной формой внутреннего мошенничества, составляя более четырех пятых известных нарушений, причем нарушения с наличными средствами и чековыми расчетами организаций равны общей доле потерь всех других активов (инвентарь, поставки, оборудование и информация). Это получение «навара» с продажи «неучтенки», незаконное списание, неприкрытое изъятие и т.д.

Коррупция, в смысле внутреннего мошенничества, обычно заключается в том, что должностное лицо, менеджер или служащий организации вступает в сговор с посторонними. Известны несколько основных типов внутренней коррупции, ведущих к ущербу для интересов предприятия: взяточничество, запрещенные денежные вознаграждения, специальное завышение цены по договоренности и пр. На долю коррупции приходится около 10% всех случаев внутреннего мошенничества.

Кто сколько ворует?

Статистические данные указывают, что приблизительно 58% известных случаев мошенничества и злоупотреблений совершаются служащими, 30% - менеджерами и 12% - топ-менеджерами и собственниками.

Семейные служащие совершают самое большое количество мошенничеств и злоупотреблений и наносят самый высокий средний ущерб – в 72% случаев. А потери, вызываемые мужчинами, в 4 раза больше потерь, вызываемых женщинами. Средние потери, вызванные виновными с высшим образованием, более чем в пять раз превышают потери, вызванные выпускниками средней школы.

Доля мошенничества с материальными ценностями непременно увеличивается в процессе роста организации, так как небольшие организации более оперативны при выявлении фактов мошенничества.

Менеджеры среднего звена образуют наиболее многочисленную группу лиц, совершающих мошенничество, хотя, в свою очередь, мошенничества, совершенные топ-менеджерами, имеют более высокую цену потерь.

Если говорить о предварительном сговоре, то он встречается более чем в 50% случаев от всех совершаемых мошенничеств, которые для предприятия-жертвы обходятся всегда намного дороже, чем другие его виды. Наиболее же чреваты последствия для предприятия, если оно оказалось жертвой сговора внутренних и внешних преступников.

Воровство.

Считается, что самое большее, на что способен обычный сотрудник – мелкое воровство: либо кража имущества родной компании, либо личных вещей коллег по работе. Расследовать и предотвращать такие преступления довольно просто. Да и ущерб от них не очень большой. Пока кто-то не украдет бумажник крупного клиента или зарубежного партнера.

Обычно, если на фирме появляется воришка, то об этом становится известно довольно быстро, и персонал сам включаются в динамичную игру «поймай вора», так как сам заинтересован в скорейшей нейтрализации этой угрозы.

А вот с «несунами» бороться труднее. Мелкие «несуны» не исчезли с распадом Советского Союза. Они и сейчас живут во многих организациях. Правда, об этом знают только их коллеги и бухгалтерия, которая регулярно списывает украденное имущество. Ущерб зависит от объема и рыночной стоимости товара, вынесенного ими за территорию организации или той сферы бизнеса, где работает компания.

Кроме того, не стоит забывать и о таком виде воровства, как использование в личных целях предоставляемых предприятием ресурсов: средств связи, оргтехники, машин и т.д. Это так же может нанести существенный урон, особенно малому предприятию.

Примеров подобного поведения может быть множество. Поэтому, никогда не помешает знать имена главных транжиров внутренних ресурсов компании.

Например, иногда таких «негативных» фактов бывает достаточно, чтобы заставить уволиться человека, которого подозревают в связях с конкурентами или криминальными структурами. Особенно если по тем или иным причинам нельзя объявить истинную причину увольнения. Такое в жизни случается значительно чаще, чем можно представить.

1.5. Первые шаги по обеспечению безопасности бизнеса

Вряд ли стоит лишний раз говорить о том, что для того чтобы свободно ориентироваться в ситуации надо обладать полной информацией о том что, где, когда и почему происходит или может произойти. Вы и сами знаете это, легко ориентируясь в том бизнесе, которым занимаетесь или хотите заняться.

В вопросах безопасности работает тот же самый принцип, и вашим первым шагом по обеспечению безопасности своего бизнеса, будет установление четкого понимания того что, где и когда может вам угрожать.

И только тогда, когда вы будете хорошо представлять, в чем состоит потенциальная опасность для вашего бизнеса, вы сможете определить возможные и доступные средства защиты и методы обеспечения безопасности.

Для этого необходимо ответить на следующие вопросы:

✓ что необходимо охранять (имущество, информацию, ценные бумаги, непосредственно персонал фирмы)?

✓ кто может представлять угрозу (преступные группы, персонал самого предприятия, спецслужбы)?

✓ как может быть осуществлена угроза (проникновение в помещение с улицы, использование персонала в корыстных целях и т.д.)?

✓ сопоставимы ли стоимость охраняемых объектов и стоимость охраны?

Прежде всего, попробуйте определить, что надо защищать и надо ли вообще что-то защищать. Определите объекты защиты.

Например, ваше предприятие занимается исключительно торговой деятельностью.

Что может подлежать защите в этом случае?

Конечно же, **товар**. Причем защита требуется всегда - в торговом зале, на складе, в дороге (при перевозке) т.д.

Но, кроме того, возможно, вы используете и свои собственные, разработанные лично вами **формы и методы продажи**. Либо за время работы, ваша **торговая марк**а стала широко известной, и сама привлекает покупателей, т.к. является гарантий высокого качества продаваемого товара.

Тогда они также должны являться объектом вашего внимания и защиты, ведь это ваше преимущество перед конкурентами.

Не стоит забывать и о работающих у вас сотрудниках.

Затем, ответьте на вопрос: **зачем**? То есть, другими словами вы определите цель построения системы безопасности предприятия и задачи, которые при этом должны решаться.

В рассматриваемом нами примере торгового предприятия ответ будет выглядеть так:

Товар – требуется обеспечение сохранности, необходимо принять меры для предотвращения кражи, порчи товара, в том числе и умышленной.

Методы продажи (и другие секреты фирмы в области работы с клиентом) – требуется защита от навязчивого интереса конкурентов. Ведь именно ваша эксклюзивность обеспечивает предприятию дополнительный доход, способствует привлечению новых клиентов.

Персонал – часто возникает необходимость обеспечения физической или психологической защиты.

Следующий вопрос, на который требуется ответить - **от кого**? Ответив на этот вопрос, вы определите источники опасности.

В рассматриваемом нами случае:

Товар требуется защищать: от **покупателей-воришек** (в торговом зале), от **небрежности персонала** (продавцов, грузчиков) - неумышленная или умышленная порча товара, от **грабителей** – в дороге. Кроме того, необходима защита и от **природных катаклизмов** – если склад, например в результате сильного ливня, будет затоплен, то вы понесете весьма ощутимые убытки.

Секреты фирмы защищаются в основном от конкурентов, но иногда требуется защита и от не в меру любопытных собственных сотрудников.

Персонал – в основном от разного рода преступных посягательств, таких как, например: вооруженное ограбление, угроза похищения или убийства, психологический террор, шантаж, вымогательство.

И, наконец, последний вопрос - **как**? Ответив на него, вы определите, методы и средства защиты. Правда иногда, для того чтобы получить ответ на этот вопрос, требуется обратиться к специалистам.

Затем, используя результаты проведенного вами анализа, вы можете приступить к планированию работ по обеспечению безопасности вашего предприятия, определить необходимые организационные и технические меры, рассчитать стоимость затрат и оценить эффективность проводимых мероприятий. При этом важно понимать, какие работы вы в состоянии выполнить собственными силами, а в каких случаях требуется прибегнуть к помощи профессионалов.

Для лучшего понимания того, что же такое система безопасности предприятия (для чего она создается, какие задачи решает, как строится) и для того чтобы в дальнейшем эффективно построить свою систему безопасности, необходимо четко определить следующие моменты:

- ✓ Конкурентная борьба
- ✓ Субъекты безопасности предприятия
- ✓ Принципы построения системы безопасности
- ✓ Средства и методы обеспечения безопасности
- ✓ Формирование Службы безопасности
- ✓ Основные функции Службы безопасности
- ✓ Правовые основы деятельности Службы безопасности и др.

ГЛАВА 2.
ПРОЦЕСС ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА РЕГИОНАЛЬНОМ УРОВНЕ

2.1. Система показателей и индикаторов экономической безопасности в регионе

Одной из первостепенных задач при изучении экономической безопасности является разработка такой системы показателей, которая объективно и своевременно отражала бы кризисные явления в экономике. Это является сложной методической проблемой, для решения которой необходимо провести классификацию существующих показателей экономической безопасности. Можно предложить следующую классификацию показателей экономической безопасности.

В связи с многообразием факторов, влияющих на экономическую безопасность и ее многоуровневую систему, существует большое количество различных показателей, характеризующих безопасность, и подходов к их формированию. Отсутствие систематизации существующих показателей затрудняет решение этой задачи. С помощью предложенной системы задача выбора нужного показателя существенно упрощается.

Рассмотрим, какое место, в предложенной классификации, займут некоторые наиболее распространенные показатели экономической безопасности.

«Общий объем инвестиций в экономику государства»: по уровню безопасности – макроэкономический, по виду показателя - количественный индикатор, по уровню влияния – внешний, по сфере безопасности – экономическая (инвестиционная). «Уровень безработицы в субъекте федерации, (%)»: по уровню безопасности – мезоуровень, по виду показателя – качественный индикатор, по уровню влияния – внутренний, по сфере безопасности – социальный (рынок труда).

«Пороговое значение отношения дефицита бюджета субъекта федерации к валовому региональному продукту субъекта федерации» - по уровню безопасности – мезоуровень, по виду показателя – качественный порог, по уровню влияния – внутренний, по сфере безопасности – экономическая (финансовая).

Такая классификация показателей отражает особенности экономической безопасности: ее сложную, многоуровневую структуру; огромное количество различных социально-экономических факторов, влияющих на нее; разнообразие существующих подходов к формированию систем показателей ее оценки. Значимость, предложенной классификации заключается в том, что она позволяет существенно упростить задачу выбора показателя (показателей), наиболее полно характеризующего ту или иную сферу экономики в зависимости от уровня безопасности. Кроме того, классификация позволяет создавать многоуровневые системы показателей, отражающих положение дел во всех сферах жизнедеятельности региона.

Представляет определённый интерес система показателей оценки экономической безопасности в регионе, предложенная группой авторов Института экономики Уральского отделения РАН (Татаркиным А.И и др.). Однако при анализе кризисных ситуаций в производственной сфере использование индикаторов, предложенной системы, не представляется возможным, в связи с их отсутствием в существующей системе статистического учета. Поэтому анализ кризисных ситуаций в производственной сфере целесообразно проводить, используя показатели по которым ведется статистический учет, а именно: объемы отгруженных товаров собственного производства, выполненных работ и услуг собственными силами по видам деятельности.

Отдельное внимание необходимо уделить методике оценки энергетической безопасности. В предлагаемой системе используется два интегральных показателя: доля собственных источников в балансе топлива и электроэнергии на территории и степень обеспечения запасами топлива у потребителей. Однако, ряд регионов Российской Федерации собственных источников в балансе топлива и электроэнергии не имеют, и особенностью таких регионов является то, что их энергетическая безопасность полностью зависит от запасов топлива. Соответственно использование первого интегрального показателя не возможно, и оценку энергетической безопасности таких регионов целесообразно проводить, ориентируясь только на обеспеченность запасами топлива. При этом пороговые значения (предкризис1 - ПК1, предкризис2 - ПК2, предкризис3 - ПК3, кризис1 - К1, кризис2 - К2, кризис3 - К3) степени обеспечения запасами топлива у потребителей целесообразно увеличить на соответствующие значения доли

Для обеспечения региональной социально-экономической безопасности (условий защищенности и обеспечения жизнедеятельности с учетом внешних и внутренних угроз) необходима система ее оценки на региональном и муниципальном уровне. Формирование индикаторов экономической безопасности региона и муниципального уровня (муниципальный район) может осуществляется по следующим сферам деятельности (см. Табл. 1).

Таблица 1

Индикаторы экономической безопасности по сферам жизнедеятельности

На региональном уровне	На муниципальном уровне
1. Способность экономики территории к устойчивому росту	
1.1. Инвестиционная безопасность	1.1. Инвестиционная безопасность
1.2. Производственная безопасность	1.2. Производственная безопасность
1.3. Научно-техническая безопасность	1.3. Безопасность собственности
1.4. Внешнеэкономическая безопасность	
1.5. Финансовая безопасность	1.4. Финансовая безопасность
1.6. Энергетическая безопасность	1.5. Энергетическая безопасность
2. Обеспечение приемлемого уровня существования на территории	
2.1. Уровень жизни населения	2.1. Социальный уровень жизни населения
2.2. Рынок труда	2.2. Рынок труда и оплата труда
2.3. Демографическая безопасность	2.3. Демографическая безопасность
2.4. Правопорядок	2.4. Правопорядок
2.5. Продовольственная безопасность	2.5. Продовольственная безопасность
3. Экологическая безопасность	
3.1. Экологическая защита	3.1 Выбросы вредных веществ

Каждая из сфер включает определенный набор индикативных показателей (обычно от 3 до 7). Их состав для каждого из уровней различен. Индикаторы экономической безопасности региона в целом существенно не отличаются от индикаторов, по которым производится диагностика экономической безопасности территорий муниципального уровня.

В условиях рыночной экономики субъекты рынка в тот или иной период могут находиться в совершенно разных взаимоотношениях. Недавнее сотрудничество быстро перерастает в противодействие. Возможен и обратный вариант, когда конкурирующие организации начинают взаимодействовать с целью обоюдного улучшения положения на рынке.

Большое значение для понимания механизмов конкурентной борьбы имеет Закон РФ *«О конкуренции и ограничении монополистической деятельности на товарном рынке»*.

Под **конкуренцией** понимается состязательность хозяйствующих субъектов, когда их самостоятельные действия эффективно ограничивают возможность каждого из них односторонне воздействовать на общие условия обращения товаров на соответствующем товарном рынке.

Конкурентная борьба на рынке дает возможность компаниям увеличивать свой доход и прибыль. Поэтому предпринимателям жизненно необходимо иметь ясное и объективное представление о своих прямых и косвенных конкурентах на рынке. А также иметь четкое представление о настоящем положении компании в отрасли.

2.2. Модель конкурентной среды М. Портера

Для проведения анализа сложившейся в отрасли ситуации широко применяется модель М. Портера. Эта модель носит название «модель пяти сил», что обусловлено выделением автором пяти основных аспектов, качественно влияющих на состояние компании. Некоторые отечественные авторы выделяют еще один аспект, к сожалению, свойственный российскому бизнесу. Это «административный и криминальный ресурс».

Рис. 1. Модель «пяти сил» М. Портера.

Сразу необходимо пояснить, что хозяйственная деятельность субъекта рынка подвержена влиянию гораздо большего количества факторов. Которые могут быть как прямые, например, уровень спроса на продукцию компании, так и косвенные, например, политическая нестабильность в мире, которая может повлечь скачок цен на определенный вид энергоресурсов, что приведет к увеличению стоимость закупочных материалов.

Это модель часто используется при проведении аналитических исследований в деловой разведке, так как она позволяет выявлять различные потенциальные угрозы в отношении фирмы и планировать собственные действия с их учетом. В соответствии с рассматриваемой моделью состояние конкуренции можно характеризовать пятью силами, управляющими конкуренцией в отрасли:

1) Угроза со стороны существующих конкурентов;

2) Угроза появления конкурентоспособных услуг или товаров-заменителей;

3) Угроза появления новых конкурентов;

4) Угроза со стороны партнеров (поставщиков сырья или комплектующих);

5) Угроза со стороны потребителей товаров или услуг.

Цель корпоративной стратегии фирмы – найти и занять такую позицию в отрасли, где фирма будет лучше всего защищена от влияния этих сил, или сама сможет оказать на них влияние.

Методика определения угроз с опорой на модель М. Портера состоит из нескольких этапов.

1) Выявление конкурентов (товары, услуги, финансы, недвижимость, кадры и т.д.);

2) Выявление юридической чистоты ваших контактов;

3) Рассмотрение влияния каждой силы на устойчивость вашего бизнеса;

4) Изучение структуры административного ресурса и оценка возможных реакций на ваши действия и действие конкурентов;

5) Проведение мониторинга для обнаружения возможности появления индикаторов (признаков) угроз, а также товаров заменителей;

6) Выявление потенциальных конкурентов;

7) Составление перечня угроз, их ранжирование.

2.3. Алгоритм обеспечения экономической безопасности в регионе

Управление безопасностью – непрерывный процесс обеспечения и защиты экономических интересов региона от внутренних и внешних угроз, обеспечиваемый путем осуществления комплекса мер, направленного на поддержание устойчивости и потенциала развития экономики региона. Основными задачами управления

безопасностью являются: оценка и выработка направлений деятельности по обеспечению экономической безопасности; разработка предложений о совершенствовании взаимодействия между участниками системы; планирование и проведение контрольных и профилактических мероприятий по безопасности.

Функционирование системы обеспечения безопасности региона можно представить в виде особого алгоритма.

Последовательное выполнение всех стадий на этапах мониторинга и управления экономической безопасности позволит не только отслеживать все негативные процессы в экономике региона, но и своевременно предотвращать все критические угрозы безопасности.

Результаты функционирования системы проявятся в следующем:

- создание единой информационной базы данных (системы индикаторов);

- определение основных угроз и разработка мер по их устранению;

- координация и методическое руководство деятельностью администраций городов и районов, государственных предприятий и учреждений региона, общественных организаций по вопросам, антикризисного управления;

- внедрение в практику органов власти принципов профессионального поведения антикризисных управляющих;

- выработка единых стандартов и методов антикризисного управления;

- разработка программ развития проблемных территорий региона.

Основными преимуществами предлагаемой системы являются:

- возможность непрерывно отслеживать негативные изменения в социально-экономических отношениях региона;

- малозатратность при ее создании и функционировании;

- стимулирование работы региональных органов власти по принципу взаимодействия государства и общества;

- высокая эффективность функционирования, за счет коллегиального принятия решений, четкого распределения ответственности за возникновение кризисных ситуаций и их нейтрализацию за конкретными ведомствами.

В связи с тем, что основным барьером на пути возникновения кризисных ситуаций в социально-экономических отношениях региона должна стать скоординированная деятельность органов власти, возникает необходимость в определении инструмента реализации ими своих функций и полномочий по обеспечению безопасности. Таким инструментом должна стать региональная целевая программа по обеспечению экономической безопасности.

Под региональной целевой программой понимается комплекс производственных, социально-экономических, организационно-хозяйственных и других мероприятий, увязанных по задачам, ресурсам и срокам осуществления и обеспечивающих эффективное решение системных проблем в сфере экономического, экологического,

социального и культурного развития региона. Именно системные проблемы в различных сферах региона и являются источником кризисных ситуаций, преодоление и предотвращение которых является главной задачей обеспечения экономической безопасности.

Анализ угроз национальной безопасности Российской Федерации, и экономической безопасности её регионов, показывает, что главные из них в настоящее время и в обозримой перспективе носят преимущественно внутренний характер и сосредоточены во внутриполитической и социально-экономической сферах.

Совокупность этих факторов, оказывая негативное воздействие на процесс развития внешней и внутренней обстановки, может дестабилизировать ситуацию и создать ряд реальных угроз безопасности нашей страны.

Национальная безопасность – способность общественной системы страны обеспечить высокий уровень стабильности, устойчивости, жизнедеятельности нации и ее конкурентные возможности во взаимоотношении с внешним миром в целях надежного существования и устойчивого безопасного развития. И от того, насколько удачно власть устраняет факторы риска, угрозы стабильности, во многом зависит эффективность системы обеспечения национальной безопасности страны.

Можно исходить из определения сущности и содержания экономической безопасности как степени защищенности государственных, национальных и местных интересов в сфере экономики от внешних и внутренних угроз, обеспеченной всеми средствами и институтами субъектов хозяйствования, включая структуры и систему показателей ее уровня.

Повышение экономической безопасности региона является необходимым условием обеспечения защиты его социально-экономических отношений от внутренних и внешних угроз.

Использование системы управления экономической безопасности региона, построенной на взаимодействии органов власти и общества, в основу которой положено распределение функций и ответственности между министерствами и ведомствами региона позволит не только предотвратить угрозы экономической безопасности региона, но и существенно улучшит социально-экономическую ситуацию в регионе.

Существующие комплексные системы показателей оценки и мониторинга экономической безопасности в регионе используемые при анализе ситуации в производственной сфере и энергетике нуждаются в усовершенствовании. Анализ кризисных ситуаций в производственной сфере целесообразно проводить, используя показатели по которым ведется статистический учет. Энергетическую безопасность регионов, не имеющих собственных источников в балансе топлива и электроэнергии целесообразно проводить, ориентируясь только на обеспеченность запасами топлива.

Укреплению экономической безопасности регионов должно способствовать совершенствование государственного регулирования экономического роста путем разработки концептуальных и программных документов межрегионального и территориального планирования, создания комплексной системы контроля над рисками, включая: проведение активной государственной антиинфляционной, валютной, курсовой, денежно-кредитной и налогово-бюджетной политики,

ориентированной на импортозамещение и поддержку реального сектора экономики; стимулирование и поддержку развития рынка инноваций, наукоемкой продукции и продукции с высокой добавочной стоимостью, развитие перспективных технологий общего, двойного и специального назначения.

Необходимо разрабатывать комплексные целевые программы по обеспечению экономической безопасности регионов. Важно отметить, что в настоящее время большинство региональных целевых программ имеют отношение к экономической безопасности, однако ни в названиях, ни в целях и задачах этих программ термин безопасность не употребляется.

2.4. Виды недобросовестной конкуренции

Недобросовестная конкуренция проявляется в форме *экономического подавления, промышленного шпионажа и физического подавления*.

1) Экономическое подавление:

✓ Срыв сделок и иных соглашений;

✓ Прекращение деятельности конкурентов с использованием административного ресурса;

✓ Подрыв репутации конкурента;

✓ Нарушение прав конкурентов;

✓ Дезорганизация производства конкурентов, переманивание ценных сотрудников и целых команд;

✓ Шантаж, компрометация руководителей;

✓ Сбивание цен на продукцию;

✓ Продажа по ценам ниже себестоимости с целью подрыва конкурента и дальнейшее вытеснение его с рынка;

✓ Установление контроля над деятельностью конкурента путем приобретения контрольного пакета его акций;

✓ Злоупотребление господствующим положением на рынке (например, завышение цен или отказ осуществлять поставки);

✓ Установление дискриминационных цен;

✓ Тайный сговор на торгах или создание «тайных» картелей.

2) Промышленный шпионаж:

✓ Физическое использование запрещенных методов съема информации (прослушивание телефонов, внедрение закладочных устройств...);

- ✓ Хищение документов;
- ✓ Несанкционированный доступ к компьютерной информации;
- ✓ Подкуп сотрудников конкурента с целью получения секретов.

Объекты промышленного шпионажа:

- ✓ Информация;
- ✓ Образцы изделий;
- ✓ Технологии;
- ✓ Отходы;
- ✓ Рецепты.

3) Физическое подавление:

- ✓ Ограбления, нападения на офисы, производственные помещения, персонал;
- ✓ Угрозы физической расправы над руководителями, персоналом, членами их семей;
- ✓ Заказные убийства, захват заложников.

ГЛАВА 3
ДЕЯТЕЛЬНОСТЬ ПО ОБЕСПЕЧЕНИЮ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

Обеспечением безопасности предприятия занимаются две группы субъектов.

Первая группа занимается этой деятельностью непосредственно на предприятии и подчинены его руководству.

Среди этой группы можно выделить *специализированные* субъекты (совет или комитет безопасности предприятия, служба безопасности, пожарная часть, спасательная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетенции).

Другую часть субъектов этой группы условно можно назвать *полуспециализированной*, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.).

Наконец, к третьей части этой группы субъектов относится *весь остальной персонал и подразделения предприятия*, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности.

Следует иметь в виду, что эффективно обеспечивать безопасность предприятия эти субъекты могут только в том случае, если цели, задачи, функции, права и обязанности будут распределены между ними таким образом, чтобы они не пересекались друг с другом.

Ко **второй** группе субъектов относятся *внешние органы и организации*, которые функционируют самостоятельно и не подчиняются руководству предприятия, но при этом их деятельность оказывает существенное (положительное или отрицательное) влияние на безопасность предприятия.

Субъектами этой группы являются:

1) Законодательные органы. Принятые на уровне Российской Федерации и субъектов Федерации законы составляют правовую основу деятельности по обеспечению безопасности предприятия;

2) Органы исполнительной власти. Принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования законов;

3) Суды. Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в т.ч. в сфере безопасности;

4) Правоохранительные органы. Такие органы осуществляют борьбу с правонарушениями, которые отрицательным образом влияют на состояние безопасности предприятия;

5) Научно-образовательные учреждения. Последние (особенно негосударственные образовательные учреждения для подготовки частных охранников и детективов) призваны обеспечить научно-методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятий.

Совершенно очевидно, что субъекты второй группы по своей инициативе подключаются эпизодически (или никогда) к деятельности предприятия по обеспечению своей безопасности. Организационной формой такого подключения может стать комплексная программа безопасности предприятия, в которой необходимо предусмотреть формы и методы этой работы. Кроме того, можно рекомендовать разработку планов структурных подразделений и всего предприятия в целом по организации взаимодействия с вышеуказанными органами и организациями.

3.1. Обеспечение экономической безопасности предприятия. Основные определения

Экономическая безопасность в ряде изданий определяется следующим образом: “это защищенность жизненно важных интересов личности, общества и государства в экономической сфере от внутренних и внешних угроз”. Ее специфика и значимость подразумеваются выделением экономической безопасности из общего понятия национальной безопасности.

В настоящее время, в условиях выхода экономики государства из периода депрессии, достижение стабильности функционирования субъектов предпринимательской и других видов деятельности является наиболее актуальной и важной задачей.

Для решения её немаловажную, если не решающую роль, играет обеспечение экономической безопасности этих субъектов.

Первоначально понятие экономической безопасности рассматривалось как обеспечение условий сохранения коммерческой тайны и других секретов предприятия. Такому трактованию экономической безопасности посвящены публикации начала 90-х годов прошлого столетия [13]. Обеспечение экономической безопасности рассматривалось прежде всего как защита информации, чему посвящены многие публикации. Проблему экономической безопасности предприятия в указанном контексте предлагалось решать исходя из предпосылки, что степень надежности всей системы сохранности информации определяется уровнем безопасности самого слабого ее звена, которым считается персонал организации.

Обеспечение экономической безопасности предприятия строилось в форме двухуровневой системы защиты информации. Первый уровень предполагал сохранность секретов силами службы безопасности организации, а второй - предусматривал формирование психологической атмосферы "бдительности и ответственности" персонала организации с помощью так называемых координаторов, назначаемых из лиц среднего руководящего звена и пользующихся среди сотрудников авторитетом. Признавая, что сохранность информации является одним из важных

аспектов экономической безопасности предприятия, необходимо отметить, что сведение проблемы экономической безопасности предприятия только к защите коммерческой тайны представляет собой слишком упрощенный вариант решения такой проблемы. Вполне очевидно, что столь узкое понимание экономической безопасности страдает чрезмерной "экономичностью" и не учитывает всего спектра влияния внешней среды как основного источника опасностей для деятельности предприятия.

Несколько позже возобладал другой подход к трактовке понятия экономической безопасности предприятия. Резкий спад производства в целом по стране, а главное - изменение экономических функций государства, которое уже не являлось основным инвестором и потребителем продукции, заставили посмотреть гораздо шире на проблему экономической безопасности предприятий. Согласно этому взгляду экономическая безопасность предприятия обусловлена влиянием внешней среды, которая в рыночной экономике все время изменяется, никогда не остается стабильной, постоянной или неизменной. Именно с позиций влияния внешней среды, защиты предприятий от ее отрицательного влияния и рассматривается содержание категории экономической безопасности предприятия, в том числе и в немногочисленных пока публикациях отечественных ученых-экономистов.

При определении понятия "экономическая безопасность" стало преобладать мнение, что его содержание отражает такое состояние предприятия, которое обеспечивает способность противостоять неблагоприятным внешним воздействиям. В этой связи экономическая безопасность предприятия стала рассматриваться намного шире — как возможность обеспечения его устойчивости в разнообразных, в том числе и в неблагоприятных условиях, которые складываются во внешней среде, вне зависимости от характера ее влияния на деятельность предприятия, масштаба и характера внутренних изменений. Так, экономическая безопасность предприятия определена как "защищенность его деятельности от отрицательных влияний внешней среды, а также как способность быстро устранить разно вариантные угрозы или приспособиться к существующим условиям, которые не сказываются отрицательно на его деятельности" [22]. Экономическая безопасность фирмы определяется совокупностью факторов, отражающих независимость, устойчивость, возможности роста, обеспечения экономических интересов и т.д.

Несколько иное понимание экономической безопасности предприятия приводит В. Тамбовцев [24], определяя ее как состояние предприятия, которое означает, что вероятность нежелательного изменения каких-либо качеств, параметров принадлежащего ему имущества и затрагивающей его внешней среды невелика (меньше определенного предела). В зависимости от того, какое сочетание параметров жизнедеятельности предприятия является для него желательным, будет меняться и конкретное наполнение понятия "нежелательные изменения". В общем случае к ним относятся те, которые отдаляют предприятие от его желаемого состояния. Приведенное понимание экономической безопасности предприятия предполагает и практически основывается на признании возможности стабильности внешней среды, с чем нельзя согласиться, поскольку именно изменчивость внешней среды следует рассматривать как ее постоянное состояние, а ее постоянство в течение некоторого времени - как временное состояние. Кроме того, в практической деятельности предприятий весьма затруднительно определить вероятность нежелательных изменений, которые еще необходимо четко сформулировать.

В рамках подхода к экономической безопасности предприятия как состоянию, определяемому влиянием внешней среды, следует отметить ресурсно-функциональный подход. Авторы этого подхода экономическую безопасность предприятия рассматривают как "состояние наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и обеспечения стабильного функционирования предприятия в настоящее время и в будущем" [23]. С этой целью Е. Олейников рассматривает совокупность процессов, протекающих в организации, со всеми их характерными особенностями и взаимосвязями, которые составляют единую родственную группу с точки зрения их функциональной роли в обеспечении экономической безопасности предприятия и, вместе взятые, играют важную роль в обеспечении экономической безопасности предприятия. В ресурсно-функциональном подходе в качестве основных направлений экономической безопасности предприятия различают семь функциональных составляющих: интеллектуально-кадровую, финансовую, технико-технологическую, политико-правовую, экологическую, информационную и силовую.

Тщательное изучение сущности ресурсно-функционального подхода к пониманию экономической безопасности предприятия позволяет отметить его основное достоинство - всеобъемлющий, комплексный характер, поскольку в рамках этого подхода исследуются важнейшие факторы, влияющие на состояние функциональной составляющей экономической безопасности предприятия, изучаются основные процессы, влияющие на ее обеспечение, проводится анализ распределения и использования ресурсов предприятия, рассматриваются экономические индикаторы, отражающие уровень обеспечения функциональной составляющей экономической безопасности предприятия, и разрабатываются меры по обеспечению максимально высокого уровня функциональной составляющей экономической безопасности предприятия.

Однако это достоинство ресурсно-функционального подхода одновременно является и его же недостатком, поскольку экономическая безопасность рассматривается очень широко - и в аспекте адаптации к влиянию внешней среды, и в аспекте ресурсной обеспеченности предприятия, и в аспекте качества реализации функций управления, таких как планирование, учет и анализ и т.д. При таком широком подходе теряется само видение экономической безопасности и, по сути, она отождествляется с самой деятельностью предприятия и ее эффективностью.

Помимо попыток определить сущность экономической безопасности предприятия, исходя из признания влияния, причем отрицательного, на его деятельность внешней среды, существуют и иные точки зрения по рассматриваемому вопросу. В качестве способов обеспечения экономической безопасности предприятия предлагается построение системы защиты его экономических интересов, в которой основное внимание уделено вопросам борьбы с недобросовестной конкуренцией, обеспечению информационной безопасности и правовой защите интеллектуальной собственности. Следует отметить неясность и недосказанность такого аспекта обеспечения экономической безопасности предприятия, как борьба с недобросовестной конкуренцией. В частности, непонятно, каким образом, в каких формах и какими способами предприятие может осуществлять борьбу с недобросовестной конкуренцией. Не снижая значения действий предприятий в этой борьбе, все-таки хотелось бы заметить, что такая борьба относится, скорее, к прерогативе государственных или региональных органов управления.

Заслуживает внимания точка зрения некоторых исследователей о необходимости защиты экономических интересов хозяйствующих субъектов. В этом вопросе важным является поиск правильного соотношения между вероятными потерями при нарушении экономических интересов предприятия и допустимой величиной затрат для предотвращения или минимизации потерь. Однако приведенная точка зрения носит несколько декларативный характер, поскольку защита экономических интересов автором сводится к защите информации, содержащей коммерческую тайну, а проблема выявления пограничного значения уровня затрат, разделяющего затраты на эффективные и неэффективные, только обозначена.

Отдельно хотелось бы сказать о подходах к экономической безопасности предприятия, которые можно назвать узкофункциональными. Речь идет о рассмотрении экономической безопасности предприятия с позиции отдельного аспекта его деятельности. Так, высказывается мнение, что важнейшим направлением формирования системы экономической безопасности, в том числе и предприятий, является создание действенного механизма финансовой безопасности. Обосновывается, что учет является одной из основных функций управления, направленной на обеспечение экономической безопасности предприятия, и именно учет исключает возможность прямых хищений без установленных законом последствий, создает информационные условия для осуществления контроля целесообразности и законности использования ресурсов в превентивном, текущем и следующем режимах и оказывает содействие предотвращению реализации угроз, которые снижают экономическую устойчивость предприятий.

Безусловно, разработка узкофункциональных направлений обеспечения экономической безопасности предприятия необходима, так как позволяет провести всесторонние и глубокие исследования выбранного аспекта деятельности предприятия и показать конкретные пути и способы обеспечения экономической безопасности предприятия в той или иной сфере его деятельности. Всем узкофункциональным подходам к обеспечению экономической безопасности предприятия присущ один, но, как представляется, очень серьезный недостаток. Авторы этих подходов зачастую исходят из разного понимания экономической безопасности предприятия. В этом случае попытки каким-то образом объединить узкофункциональные направления обеспечения экономической безопасности предприятия заранее обречены на неудачу. Отсутствие единого понимания экономической безопасности предприятия может значительно снизить результативность узкофункционального подхода, т. е. попросту обесценить ее, хотя такой подход в целом ряде случаев может принести ощутимую пользу.

Анализ рассмотренных подходов к проблеме экономической безопасности предприятия позволяет сделать следующие выводы. Экономическая безопасность предприятия складывается из нескольких функциональных составляющих, которые для каждого конкретного предприятия могут иметь различные приоритеты в зависимости от характера существующих угроз. Основным фактором, определяющим состояние экономической безопасности является обладание предприятием устойчивыми конкурентными преимуществами. Эти преимущества должны соответствовать стратегическим целям предприятия. На основании сделанных выводов можно сформулировать собственное определение: Экономическая безопасность предприятия – это наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и

организационной структуры предприятия его стратегическим целям и задачам. Под экономической безопасностью предприятия (фирмы, организации) понимают защищенность научно-технического, технологического, производственного и кадрового потенциала от внешних и внутренних экономических угроз и способность к воспроизводству при эффективном использовании всех его ресурсов.

3.2. Причины дестабилизации экономической безопасности

Уровень экономической безопасности предприятия зависит, прежде всего, от способности руководства предвидеть и предотвратить возможные угрозы, а также быстро разрешить возникшие проблемы.

Среди причин, дестабилизирующих состояние экономической безопасности, можно выделить следующие:

- **субъективные**, вызванные неэффективной работой предприятия или его руководства, например: низкая конкурентоспособность, а, следовательно, и невостребованность продукции на рынке, действия определенных субъектов хозяйствования, неустойчивость финансового положения предприятия;

- **объективные**, возникшие не по вине конкретного предприятия, например: неспособность государства оплачивать продукцию для своих нужд, высокий уровень инфляции, форс-мажорные обстоятельства и другие.

Функциональные составляющие экономической безопасности состоит из следующих элементов:

-технико-технологическая составляющая;

-интеллектуальная и кадровая;

-финансовая;

-политико-правовая;

-экологическая;

-силовая составляющая.

Финансовая составляющая. Она является наиболее важной, поскольку финансовая стабильность говорит об обеспеченности предприятия собственными финансовыми ресурсами, уровне их использования, направлении размещения. Финансовая стабильность имеет тесную связь с эффективностью производства, а также с конечными результатами деятельности предприятия.

Причинами утраты хозяйствующим субъектом финансовой стабильности являются: уменьшение объемов производства, убыточная деятельность, высокая себестоимость продукции, неэффективное планирование и управление активами, форс-мажорные обстоятельства.

Для поддержания стабильности необходимо использовать финансовую стратегию, то

есть планирование конкретных заданий и путей их реализации в процессе финансово-экономической деятельности предприятия (фирмы, организации). Можно выделить следующие стратегические цели: усовершенствование своей продукции, снижение себестоимости, достижение эффективности производства при наименьших затратах, обеспечение достаточного уровня рентабельности.

Интеллектуальная и кадровая составляющая. В современных экономических условиях уровень экономической безопасности в большой мере зависит от квалификации и профессионализма кадров. Поэтому на предприятии должна быть создана гибкая структура управления, организована система подбора, найма, обучения и мотивации труда работников.

Управленческому персоналу предприятия необходимо постоянно анализировать состояние экономической безопасности, и он также должен быть обучен действиям в условиях возникновения кризисных ситуаций.

Технико-технологическая составляющая. При обеспечении экономической безопасности руководству необходимо анализировать, соответствуют ли применяемые на предприятии технологии современным мировым стандартам, какие технологии используются на других предприятиях, изготовляющих аналогичную продукцию; осуществлять поиск внутренних резервов улучшения используемых технологий, следить за новыми научными разработками.

Политико-правовая составляющая. Процесс охраны осуществляют по типовой схеме:

- анализ угроз негативных влияний;

- оценка текущего уровня обеспечения;

- планирование комплекса мероприятий по повышению этого уровня.

Негативные влияния можно разделить на внутренние и внешние. При анализе внутреннего влияния необходимо учитывать, насколько достаточен квалификационный уровень работников юридической службы, на каком уровне финансируется юридическое обеспечение.

При негативном внешнем влиянии причинами возникновения нестабильности могут быть политические (военные конфликты, экономические и политические блокады и т. д.) и законодательно-правовые.

Информационная составляющая. Организация или предприятие должно иметь в своем составе определенные службы, которые занимались бы накоплением и защитой информации. Целью этих служб является накопление всей необходимой информации, касающейся деятельности того или иного субъекта хозяйствования (информация, обо всех видах рынков, необходимая техническая информация, о тенденциях развития национальной и мировой экономики). После накопления полученные данные должны быть проанализированы, и результатом этого анализа должен стать прогноз тенденций развития научно-технических, экономических и политических процессов на предприятии.

На предприятии должна быть организована строгая система доступа к информации, которая включала бы в себя следующие мероприятия:

- обеспечение парольного входа в систему базы данных: регистрация, назначение и изменение паролей;

- определение прав доступа групп лиц и отдельных лиц, то есть определение допустимых операций над данными;

- тестирование средств защиты данных;

- фиксация попыток несанкционированного доступа к информации;

- исследование возникающих случаев нарушения защиты данных и проведение мероприятий по их предотвращению.

Экологическая составляющая. Для того, чтобы субъект хозяйствования был защищен от потерь, возникающих по причине штрафных санкций за нарушение экологических норм, закрытия рынков сбыта продукции предприятия в других странах с более жесткими нормами экологической чистоты товара, он должен придерживаться национальных и международных норм минимального допустимого содержания вредных веществ, попадающих в окружающую среду, а также следить за экологическими параметрами своей продукции.

Силовая составляющая. Предприятие должно быть защищено физически, то есть должен быть защищен его персонал, прежде всего руководители, имущество. Служба безопасности должна быть всегда готова к преодолению любой критической ситуации, вызванной как криминальными мотивами, так и ведением нечестной конкурентной борьбы со стороны других хозяйствующих субъектов.

Проанализировав все функциональные составляющие, можно сделать вывод, что для обеспечения экономической безопасности предприятия (организации, фирмы) от влияния субъективных и объективных причин, руководству необходимо принимать решения с такой же скоростью, с которой возникают негативные изменения, и уметь их предвидеть.

3.3. Классификация угроз

Категория «угроза» имеет не меньшее значение в теории национальной безопасности, чем категория «жизненно важные интересы». Своевременное обнаружение угроз и реагирование на них со стороны системы обеспечения национальной безопасности имеют первостепенную важность в практической деятельности по защите жизненно важных интересов личности, общества и государства. Характер и уровень угроз определяют основные направления деятельности по их предупреждению и локализации, формы, способы, средства и методы решения задач обеспечения национальной безопасности при рациональном использовании имеющихся ограниченных ресурсов.

Угроза безопасности - это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Угрозы безопасности имеют объективный характер и возникают в результате

столкновения интересов индивидов, слоев общества, классов, государств при их взаимодействии в процессе общественного развития.

Важную роль в практической деятельности по обеспечению национальной безопасности играет классификация угроз безопасности по определенным критериям на отдельные виды, что помогает улучшить организацию противодействия угрозам с учетом их конкретных особенностей. Наиболее значимыми в этом отношении критериями являются: местонахождение источника опасности; степень сформированности угрозы; характер угрозы; сферы и области человеческой деятельности; уровень субъективных оценок угроз.

Угроза может быть внешней или внутренней в зависимости оттого, где расположен источник опасности.

По степени сформированности угрозы подразделяются на потенциальные и реальные, отражая философские категории действительности и возможности.

В зависимости от характера угроз, определяемого их источником и спецификой, угрозы делятся на природные, антропогенные и социальные.

Особую практическую значимость имеет классификация угроз безопасности по сферам и областям человеческой деятельности (рисунок 2).

Подобное деление угроз имеет важное значение при организации системы обеспечения национальной безопасности и определении основных направлений ее функционирования. При этом выделение видов угроз по данному критерию можно конкретизировать для каждой самостоятельной сферы человеческой деятельности.

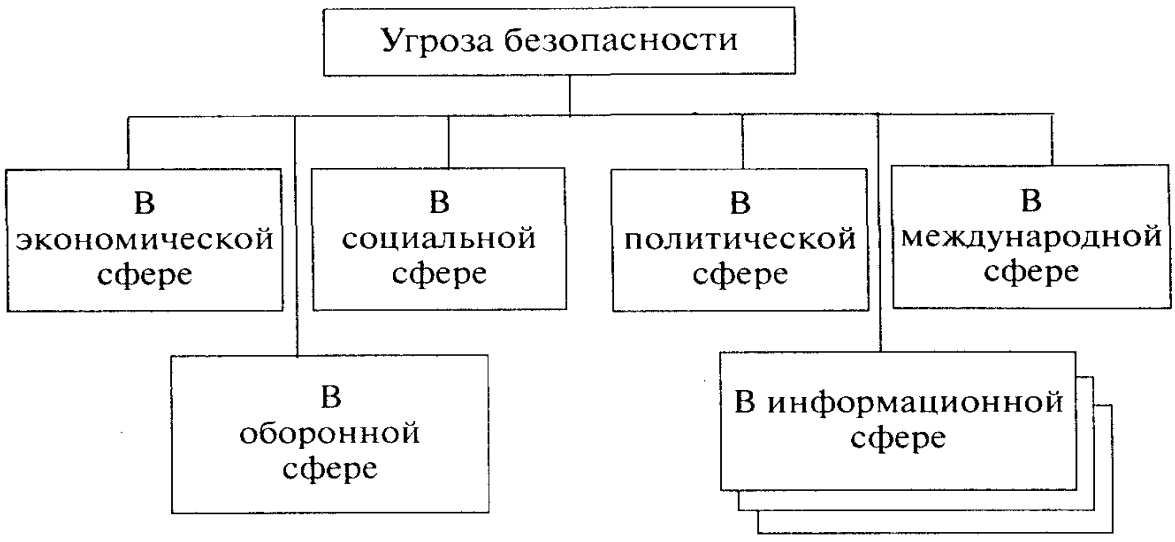


Рисунок 2. Классификация угроз безопасности по сферам и областям человеческой деятельности

Угроза национальной безопасности (интересам личности, общества и государства) представляет собой посягательство на интерес. Угрозы интересам существуют в каждой сфере жизнедеятельности. Они таятся вне и внутри личности, общества и государства.

В целом все выделенные выше по различным критериям виды угроз оказывают большое влияние на формирование, развитие и практическую деятельность системы обеспечения национальной безопасности России.

Состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, социально-политическая поляризация российского общества и криминализация общественных отношений, рост организованной преступности и увеличение масштабов терроризма, обострение межнациональных и осложнение международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности страны.

В сфере экономики угрозы имеют комплексный характер и обусловлены прежде всего сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и предметов потребления, включая предметы первой необходимости.

3.4. Механизм реализации угроз

Исходя из того, что основой возникновения угроз являются взаимодействия различных элементов вне и внутри предприятия, то эти элементы могут являться источниками угроз, а также объектами угроз. В процессе обеспечения экономической безопасности эти же элементы вне и внутри предприятия могут рассматриваться как объекты обеспечения экономической безопасности и субъекты (средства, механизмы, способы и т.д.) обеспечения экономической безопасности. Эти рассуждения и анализ практики предприятий позволяет сформулировать следующий принцип.

Любой элемент вне и внутри предприятия с точки зрения обеспечения безопасности предприятия может выступать одновременно в четырех аспектах:

- ✓ субъекта (средство, механизм, способ) обеспечения безопасности;
- ✓ объекта обеспечения безопасности (защищаемый элемент);
- ✓ источника угрозы;
- ✓ объекта угрозы.

Итак, ко внешним угрозам и дестабилизирующим факторам можно отнести противоправную деятельность криминальных структур, конкурентов, фирм и частных лиц, занимающихся промышленным шпионажем либо мошенничеством, несостоятельных деловых партнеров, ранее уволенных за различные проступки сотрудников предприятия, а также правонарушения со стороны коррумпированных элементов из числа представителей контролирующих и правоохранительных органов.

К внутренним угрозам и дестабилизирующим факторам относятся действия или бездействия (в том числе умышленные и неумышленные) сотрудников предприятия,

противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба компании, утечка или утрата информационных ресурсов (в том числе сведений, составляющих коммерческую тайну и/или конфиденциальную информацию), подрыв ее делового имиджа в бизнес-кругах, возникновение проблем во взаимоотношениях с реальными и потенциальными партнерами (вплоть до утраты важных контрактов), конфликтных ситуаций с представителями криминальной среды, конкурентами, контролирующими и правоохранительными органами, производственный травматизм или гибель персонала и т.д. Выделяют внешнюю и внутреннюю экономическую безопасности.

Под внутренней составляющей экономической безопасности предприятия будем понимать свойство (способность) предприятия организовывать свою внутреннюю структуру и взаимоотношения внутри предприятия таким образом, чтобы максимально обеспечить свою экономическую безопасность. Таким образом, понятие внутренней экономической безопасности характеризует степень того, насколько внутреннее устройство предприятия способствует обеспечению экономической безопасности в целом в целом.

Под внешней составляющей экономической безопасности понимается свойство (способность) предприятия организовывать взаимоотношения с внешней средой таким образом, чтобы максимально обеспечить свою экономическую безопасность.

Следует отметить, что обе эти составляющие экономической безопасности теснейшим образом связаны между собой и такое деление довольно условно. Что немаловажно, внутренняя составляющая экономической безопасности имеет первостепенное значение. К этому можно прийти путем следующих рассуждений. Будем рассматривать более или менее одинаковые предприятия, находящиеся в одной и той же внешней среде. Если у них могут быть разные уровни обеспечения экономической безопасности, то это может быть обусловлено только «внутренним устройством» данных предприятий. Следовательно, внутренняя составляющая экономической безопасности в значительной мере или даже полностью определяет и внешнюю составляющую экономической безопасности.

3.5. Задачи экономической безопасности

В современных условиях процесс успешного функционирования и экономического развития российских предприятий во многом зависит от совершенствования их деятельности в области обеспечения экономической безопасности. Следует заметить, что сегодня не все руководители предприятий готовы в полной мере оценить важность создания надежной системы экономической безопасности. Экономическая безопасность предприятия — это состояние его защищенности от негативного влияния внешних и внутренних угроз, дестабилизирующих факторов, при которых достигается устойчивая реализация главных коммерческих интересов и целей уставной деятельности.

Для каждого предприятия «внешние» и «внутренние» угрозы сугубо индивидуальны. Ко внешним угрозам и дестабилизирующим факторам можно отнести противоправную деятельность криминальных структур, конкурентов, фирм и частных лиц,

занимающихся промышленным шпионажем либо мошенничеством, несостоятельных деловых партнеров, ранее уволенных за различные проступки сотрудников предприятия, а также правонарушения со стороны коррумпированных элементов из числа представителей контролирующих и правоохранительных органов. К внутренним угрозам и дестабилизирующим факторам относятся действия или бездействие сотрудников предприятия, противоречащие интересам его коммерческой деятельности, следствием которых могут быть нанесение экономического ущерба компании, утечка или утрата информационных ресурсов, подрыв ее делового имиджа в бизнес-кругах, возникновение проблем во взаимоотношениях с реальными и потенциальными партнерами, конфликтные ситуаций с представителями криминальной среды, конкурентами, контролирующими и правоохранительными органами, производственный травматизм или гибель персонала и т.д.

К числу основных задач системы экономической безопасности любой коммерческой структуры относятся:

✓ защита законных прав и интересов предприятия и его сотрудников;

✓ сбор, анализ, оценка данных и прогнозирование развития обстановки;

✓ изучение партнеров, клиентов, конкурентов, кандидатов на работу в компании;

✓ своевременное выявление возможных устремлений к предприятию и его сотрудникам со стороны источников внешних угроз безопасности;

✓ недопущение проникновения на предприятие структур экономической разведки конкурентов, организованной преступности и отдельных лиц с противоправными намерениями;

✓ противодействие техническому проникновению в преступных целях;

✓ выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников предприятия в ущерб его безопасности;

✓ защита сотрудников предприятия от насильственных посягательств;

✓ обеспечение сохранности материальных ценностей и сведений, составляющих коммерческую тайну предприятия;

✓ добывание необходимой информации для выработки наиболее оптимальных управленческих решений по вопросам стратегии и тактики экономической деятельности компании;

✓ физическая и техническая охрана зданий, сооружений, территории и транспортных средств;

✓ формирование среди населения и деловых партнеров благоприятного мнения о предприятии, способствующего реализации планов экономической деятельности и уставных целей;

✓ возмещение материального и морального ущерба, нанесенного в результате неправомерных действий организаций и отдельных лиц;

✓ контроль за эффективностью функционирования системы безопасности,

совершенствование ее элементов.

С учетом перечисленных задач, условий конкурентной борьбы, специфики бизнеса предприятия строится его система экономической безопасности. Необходимо отметить, что система экономической безопасности каждой компании также сугубо индивидуальна. Ее полнота и действенность во многом зависят от имеющейся в государстве законодательной базы, выделяемых руководителем предприятия материально-технических и финансовых ресурсов, понимания каждым из сотрудников важности обеспечения безопасности бизнеса, а также от знаний и практического опыта начальника системы экономической безопасности, непосредственно занимающегося построением и поддержанием в «рабочем состоянии» самой системы.

ГЛАВА 4
ФИНАНСОВО-ХОЗЯЙСТВЕННАЯ ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ

Количественный и качественный анализ перечисленных выше угроз позволяет сделать вывод о том, что надежная защита любой компании возможна только при **комплексном и системном подходе** к ее организации. В связи с этим в лексиконе профессионалов, занимающихся обеспечением безопасности бизнеса коммерческих структур, появился термин **«система безопасности»** предприятия.

Системой безопасности предприятия является комплекс организационно-управленческих, режимных, технических, профилактических и пропагандистских мер, направленных на качественную реализацию защиты интересов предприятия от внешних и внутренних угроз.

Целью создания системы безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее организации:

1) успешно функционировать в нестабильных условиях внешней и внутренней среды;

2) предотвращать угрозы собственной безопасности;

3) защищать свои законные интересы от противоправных посягательств;

4) охранять жизнь и здоровья персонала;

5) не допускать хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации.

К числу **основных задач системы безопасности** любой коммерческой структуры относятся:

✓ защита законных прав и интересов предприятия и его сотрудников;

✓ сбор, анализ, оценка данных и прогнозирование развития обстановки;

✓ изучение партнеров, клиентов, конкурентов, кандидатов на работу в компании;

✓ своевременное выявление возможных устремлений к предприятию и его сотрудникам со стороны источников внешних угроз безопасности;

✓ недопущение проникновения на предприятие структур экономической разведки конкурентов, организованной преступности и отдельных лиц с противоправными намерениями;

✓ противодействие техническому проникновению в преступных целях;

✓ выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников предприятия в ущерб его безопасности;

✓ защита сотрудников предприятия от насильственных посягательств;

✓ обеспечение сохранности материальных ценностей и сведений, составляющих коммерческую тайну предприятия;

✓ добывание необходимой информации для выработки наиболее оптимальных управленческих решений по вопросам стратегии и тактики экономической деятельности компании;

✓ физическая и техническая охрана зданий, сооружений, территории и транспортных средств;

✓ формирование среди населения и деловых партнеров благоприятного мнения о предприятии, способствующего реализации планов экономической деятельности и уставных целей;

✓ возмещение материального и морального ущерба, нанесенного в результате неправомерных действий организаций и отдельных лиц;

✓ контроль за эффективностью функционирования системы безопасности, совершенствование ее элементов.

Результатом деятельности по обеспечению комплексной безопасности предприятия являются: стабильность (надежность) его функционирования и финансово-экономического состояния, личная безопасность персонала.

4.1. Принципы построения системы безопасности предприятия

С учетом перечисленных задач, условий конкурентной борьбы, специфики бизнеса предприятия строится его система безопасности. Необходимо отметить, что система безопасности каждой компании также сугубо индивидуальна. Ее полнота и действенность во многом зависят от имеющейся в государстве законодательной базы, выделяемых руководителем предприятия материально-технических и финансовых ресурсов, понимания каждым из сотрудников важности обеспечения безопасности бизнеса, а также от знаний и практического опыта начальника службы безопасности (СБ), непосредственно занимающегося построением и поддержанием в «рабочем состоянии» самой системы.

Система безопасности предприятия может быть построена на основе следующих **принципов**:

1) Приоритет мер предупреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз;

2) Законность. Меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам;

3) Комплексное использование сил и средств. Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является **программа обеспечения безопасности** предприятия;

4) Координация и взаимодействие внутри и вне предприятия. Меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может комитет (группа совет и т.д.) безопасности предприятия;

5) Сочетание гласности с конспирацией. Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль - предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6) Компетентность. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям;

7) Экономическая целесообразность. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения;

8) Плановая основа деятельности. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников;

9) Системность. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

Особенностью и, одновременно, сложностью при построении системы корпоративной безопасности является тот факт, что ее действенность практически полностью зависит от **человеческого фактора**. Как показывает практика, даже при наличии на предприятии профессионально подготовленного начальника службы безопасности, современных технические средств, вы не добьетесь желаемых результатов до тех пор, пока в вашем коллективе каждый сотрудник не осознает важность и необходимость внедряемых мер корпоративной безопасности.

А они будут не популярны:

✓ кто-то утратит возможность в рабочее время или после работы развлекаться в Интернете, скачивать музыку и иную информацию, читать книги в электронном варианте и т.д.;

✓ кому-то покажется в тягость один раз в неделю менять пароль на своем компьютере;

✓ кто-то посчитает ниже своего достоинства всякий раз подниматься для того, чтобы уничтожить черновик в бумагорезательной машинке, убрать со стола документы и закрыть окно после окончания рабочего дня, опечатывать и сдавать свой рабочий кабинет под роспись в журнале службе охраны;

✓ у кого-то исчезнет возможность приводить на работу (в том числе и по выходным дням) своих друзей, либо похвалиться на стороне личными достижениями в работе или успехами фирмы;

✓ некоторые не смогут использовать служебные автотранспорт и мобильный телефон в личных целях, а также часами вести личные разговоры по служебным проводным каналам телефонной связи и т.д.

Поэтому для юридически правильного, эффективного и всестороннего использования системы безопасности в защите интересов предприятия от всех видов недоброжелателей требования по обеспечению безопасности бизнеса излагаются в соответствующих **приказах** руководителя, **трудовых договорах** с сотрудниками и их **должностных обязанностях**, специальных **инструкциях**, **положениях**, **контрактах** с деловыми партнерами и т.д. После чего доводятся до персонала под роспись в процессе занятий и инструктажей.

В вопросах безопасности предприятия как никогда важна роль и понимание актуальности проблемы в первую очередь самим руководителем предприятия.

Директор и, при наличии, начальник службы безопасности, должны пропагандировать среди персонала **одно из основных корпоративных правил:** *«Фирма – это твоя вторая семья. Предприятие дает всем сотрудникам работу, материальные блага, перспективы служебного роста и т.д. В связи с этим задача каждого сотрудника – приумножать успех и материальное положение компании (как и своей семьи). Ведь успех предприятия – это стабильность и перспективы его персонала».*

Вместе с тем, как показывает практика, кто-то из ваших сотрудников может не выполнять установленные в компании требования или допускать ошибки по забывчивости, кто-то по неаккуратности, а кто-то – из мести. У кого-то могут возникнуть финансовые затруднения в связи с болезнью близких или в связи с проигрышем в казино, и он решит их «компенсировать» за счет фирмы. Кто-то посчитает, что был незаслуженно наказан директором, что давно достоин повышения в должности или что его вклад в деятельность компании заслуживает гораздо более высокой зарплаты, а руководство этого не замечает и т.д.

Словом, с возрастом, изменением социального статуса, материального благосостояния, появлением вредных наклонностей, а также при возникновении некоторых объективных обстоятельств люди могут меняться либо вести себя неадекватно. При этом необходимо понимать, что в вопросах обеспечения безопасности «второстепенных» должностных лиц нет, а есть только особенности (в связи с выполняемыми каждым из сотрудников функциями и обязанностями).

Секретарь обладает серьезным объемом самой разноплановой информации о фирме.

Уборщица может похитить с рабочего стола директора документ с важной

информацией или переписать, запомнить, ксерокопировать его содержание, добросовестно выбросить из мусорной корзины не уничтоженные документы либо документы, уничтоженные таким образом, что не составляет никакого труда их восстановить.

Охранник в состоянии сделать все то же самое, а в ночное время и выходные дни у него появляется дополнительная возможность впустить в офис посторонних, которые, в свою очередь, могут вам навредить (начиная от банального хищения документов и имущества и заканчивая постановкой в Вашем кабинете подслушивающей техники или «перекачки» закрытой информации из вашего компьютера).

4.2. Классификация элементов финансово-хозяйственной деятельности

Поскольку нам необходимо вести плановую деятельность по обеспечению безопасности предприятия, то перед нами неизбежно возникает задача систематизации этой деятельности. Как мы уже выяснили, среди принципов организации таковой деятельности существенное место занимает системность. На практике это означает, что обязательно должен существовать и применяться инструмент (технология, способ), позволяющий управлять процессом обеспечения безопасности. Этот инструмент должен:

✓ быть универсальным по отношению к большинству предприятий;

✓ учитывать все или большинство индивидуальных особенностей предприятий;

✓ давать наглядное представление о системе безопасности предприятия;

✓ позволять формализовывать деятельность по обеспечению безопасности предприятий;

✓ позволять вести и оценивать деятельность по обеспечению безопасности предприятия в соответствии с определенными стандартами;

✓ быть простым и доступным для понимания и использования.

В качестве такого инструмента можно предложить составление и использование матриц (таблиц) обеспечения безопасности предприятия.

Любое событие финансово-хозяйственной деятельности предприятия, включая также угрозу экономической безопасности, и мероприятия по предотвращению ее реализации могут быть классифицированы в соответствии с принципом шести уровней. Кроме того, каждое событие финансово-хозяйственной деятельности предприятия может быть отнесено к какому-либо из видов (аспектов) деятельности или соответствующему виду безопасности. При этом путем экспертной оценки, учета пожеланий руководства, учредителей, предыдущего опыта, научно-практических работ в данной области, а также на основе анализа финансово-хозяйственной деятельности эти виды безопасности можно ранжировать, например, в порядке убывания важности для предприятия.

Каждое событие финансово-хозяйственной деятельности предприятия, каждый его

элемент у нас классифицируется по двум признакам: уровню в финансово-хозяйственной деятельности и виду безопасности.

4.3. Информация о финансово-хозяйственной деятельности предприятия, как основа безопасности

Экономическая безопасность выше на тех предприятиях (фирмах), которые не только знают, что должно быть произведено, где и по какой цене продано, но и как рационально организовывать свой бизнес, чтобы достичь поставленных целей с наименьшими издержками и потерями. Осуществляя руководство предприятием (фирмой), необходимо принимать во внимание всю совокупность управляемых параметров (инструментов маркетинга) и ограничений внешней среды. Поэтому к сфере управления экономической безопасностью относятся также вопросы стабильной работы предприятия (фирмы), связанные с формированием затрат и цен на готовую продукцию, с кругооборотом средств предприятия, с образованием и расходованием его материальных, трудовых и финансовых ресурсов, с обеспечением расчетов с деловыми партнерами, банками, бюджетом.

Все это производится на языке бизнеса, т.е. в рамках единого системного бухгалтерского учета. До недавнего времени в отечественной теории и практике было не принято выделять в рамках единого учета такие его классификационные группы, как финансовый и управленческий учет [28]. Вместе с тем в рыночных экономических системах существует ряд объективных причин с учетом обеспечения экономической безопасности, в силу которых единый системный учет целесообразно подразделять на его «финансовую» и «управленческую» составляющие. Прежде всего это причины организационно-информационного характера.

Основной задачей бухгалтерского учета на предприятии (фирме), работающем в условиях рынка, является своевременное обеспечение многочисленных пользователей специфической экономической информацией. Достоверная экономическая информация помогает в условиях неопределенности и риска принимать ответственные и эффективные управленческие решения, способные самым существенным образом повлиять на будущее финансовое положение предприятия, на материальное благосостояние его собственников (акционеров), его руководителей (менеджеров) и наемных работников, а также на величину поступления средств в государственный бюджет.

Вся совокупность информации, формируемая учетно-аналитической функцией на любом предприятии (фирме), подразделяется на следующие основные категории.

1. Информация, которая необходима для эффективного управления предприятием (фирмой). Она используется руководством (менеджерами) и служит для обеспечения текущего и оперативного управления производственно-хозяйственной деятельностью и контроллинга. Эта информация включает данные о величине затрат на производство и реализацию продукции, себестоимости единицы продукции, величине ожидаемых доходов и расходов в результате осуществления планируемых хозяйственных и маркетинговых операций, контрактов, сделок, инвестиций, прогнозирование сбыта и уровня рентабельности товаров рыночной новизны, находящихся в стадии освоения

выпуска.

Эта информация формируется в рамках управленческого (или производственного) бухгалтерского учета. В большинстве случаев она относится к сведениям, составляющим коммерческую тайну. Как правило, внутри самого предприятия объем управленческой информации для руководителей различных уровней ограничен лишь рамками их непосредственной компетенции. Доступ к различным видам иной управленческой информации, которая не связана с осуществлением ими своих функциональных обязанностей, зачастую бывает ограничен.

2. Информация, которая отражает текущее финансовое состояние предприяти, величину и структуру его активов (имущества) и источников их образования, размер вовлеченных в оборот материальных и финансовых ресурсов и эффективность их использования и т.д.

Формирование такого рода информации осуществляется в рамках финансового бухгалтерского учета. Часть этой информации может тоже составлять коммерческую тайну. Финансовая же отчетность стандартизована и составляется в строгом соответствии со специальными общепринятыми государственными требованиями, и доступ к ней, как правило, свободен, Эта информация используется также и для внутрифирменного управления руководством предприятия и менеджерами различных уровней, обеспечивающими его экономическую безопасность.

Несмотря на имеющиеся отличительные особенности управленческого и финансового учета, следует иметь в виду их единую основополагающую функцию в общей системе управления предприятием и в едином процессе принятия управленческих решений. Такой функцией является информационное (перспективное и/или ретроспективное) отражение экономического и финансового состояния предприятия через систему специальных показателей.

В международной практике поменяется множество показателей, определяющих финансовую стабильность предприятия как составную часть экономической безопасности. Это и ранее известные по технико-экономический обоснованиям такие показатели, как рентабельность, коэффициент ликвидности (широко применяется в Японии), коэффициент эффективности капвложений, срок окупаемости и т.д. Американские специалисты часто используют показатели чистой приведенной величины дохода, максимальных денежных потоков (кэш-флоу) и особенно маржи безопасности или точки безубыточности и др.

Для расчета всех необходимых экономических показателей, наиболее полно характеризующих состояние экономической безопасности предприятия, необходимо разработать ряд следующих документов, у каждого из которых свое назначение:

✓ прогноз объемов реализации (продаж) призван дать представление о той доли рынка, которую предполагает занять выпускаемая предприятием (фирмой) продукция;

✓ баланс денежных расходов и поступлений, т.е. определение суммарных доходов и расходов, связанных с реализацией конкретного вида продукции на базе «ноу-хау» (коммерческой тайны), уточнение необходимости привлечения заемных средств, проверки синхронности поступления и расходования денежных средств. Таким образом, данный документ позволяет проверить будущую ликвидность предприятия

(фирмы) и рассчитать маржу безопасности;

✓ сводный баланс активов я пассивов (финансовая ведомость), который позволяет оценить, какие суммы намечается вложить в активы разных типов и за счет каких пассивов предприятие (фирма) собирается финансировать создание или приобретение этих активов.

Таким образом, данный баланс является как бы индикатором финансового положения предприятия (фирмы), его платежеспособности.

По отдельным показателям финансового состояния предприятия (фирмы) в мировой практике определились нормативы оптимальных величин экономической безопасности [28].

Например, соотношение собственных и заемных средств должно быть в пропорции 1:1, ликвидность — на уровне 1 и выше, коэффициент покрытия краткосрочных обязательств оборотными средствами — 2, обеспеченность недвижимостью — приближающаяся к 1, а чистая рентабельность капитала — выше процента за банковский кредит.

Одним из показателей платежеспособности служит показатель отношения оборотных средств к краткосрочной задолженности. На практике это соотношение должно составлять 2:1, что означает, что краткосрочные обязательства дважды перекрываются активами.

Другим показателем платежеспособности предприятия (фирмы) является отношение долгосрочной задолженности к собственному капиталу фирмы. В норме это соотношение должно составлять 0,65 и меньше.

Недвижимость обеспечивает финансовую устойчивость предприятия (фирмы) и свидетельствует об удельном весе стоимости основных фондов, финансовых ресурсов и имущественных прав в совокупных активах предприятии. Оптимальный показатель - 0,5. Обеспеченность недвижимостью достигается при равенстве показателя недвижимости и собственного капитала. Нормативное значение - 1. Увеличение величины показателя говорит об устойчивости и платежеспособности предприятия.

Рассмотрим методику анализа финансовой деятельности предприятия за отчетный период с помощью относительных финансовых коэффициентов. Эти коэффициенты можно разбить на три группы. В первую группу входят коэффициенты ликвидности оборотных средств K1 и K2, где

$$K_1 = \frac{Оборотные_активы}{Оборотные_пассивы}$$

$$K_2 = \frac{Оборотные_активы - Товарные_запасы}{Оборотные_пассивы}$$

Если коэффициент K1 характеризует ликвидность оборотных средств, то коэффициент K2 - быстроту ликвидности оборотных средств. В мировой практике для успешно работающих предприятий промышленности рекомендуются: k1 > 1,8 и K2 > 1,0. Эти коэффициенты ограничивают затоваривание предприятия готовой продукцией.

Во вторую группу коэффициента входят коэффициент К3, характеризующий оборот товарных запасов, и К4, характеризующий эффективность использования абсолютных активов. Они оцениваются по следующим формулам:

$$К_3 = \frac{\text{Суммарные затраты на производство и реализацию товаров}}{\text{Стоимость товаров}}$$

$$К_4 = \frac{\text{Доход от продажи товаров}}{\text{Стоимость запаса товаров}}$$

В мировой практике для успешно работающих промышленных предприятий рекомендуются: К3 > 2,8 и К4 > 1,6.

К третьей группе показателей относятся коэффициенты прибыльности К5 и К6, где

$$К_5 = \frac{\text{Прибыль до вычита налога}}{\text{Доход от продажи товаров}} \times 100\%$$

$$К_6 = \frac{\text{Прибыль до вычита налога}}{\text{Абсолютные активы}} \times 100\%$$

В мировой практике для успешно работающих промышленных предприятий рекомендуются: К5 > 8,2% и К6 > 14,7%

Для малых предприятий и фирм (активы от 1 до 10 млн. долл.) рекомендуются следующие значения этих коэффициентов:

К1 > 1,8, К2 > 0,9, К3 > 3,2, К4 > 1,7; К5 > 6,7%; К6 > 15 %.

При анализе финансовой деятельности предприятия с помощью этих коэффициентов можно использовать следующие рекомендации:

1. Если значения всех коэффициентов выше приведенных цифр, то можно сделать вывод, что предприятие работает эффективно.

2. Если значение какого-либо из коэффициентов несколько ниже рекомендованного уровня, то он должен быть под постоянным контролем со стороны руководства предприятия.

3. Если значения коэффициентов К3 и К4 ниже рекомендованных уровней, то руководству предприятия следует проанализировать продуктивность всех статей актива, эффективность маркетинговых мероприятий.

В случае, если большинство коэффициентов будет существенно ниже рекомендованных уровней, необходимо серьезно заняться анализом всей финансовой деятельности предприятия.

При анализе финансового состояния предприятия представляет также интерес показатель вероятности банкротства Z, который отражает финансовую устойчивость предприятия. Он оценивается по следующей формуле:

$$Z = 1{,}2 \times \frac{\text{Оборотные активы}}{\text{Абсолютные активы}} + 1{,}4 \times \frac{\text{Нераспределенная прибыль}}{\text{Абсолютные активы}} +$$
$$+ 0{,}6 \times \frac{\text{Рыночная стоимость обычных и привилегированных акций}}{\text{Абсолютные активы}} +$$
$$+ 3{,}3 \times \frac{\text{Доход от основной деятельности}}{\text{Абсолютные активы}} + 1{,}0 \times \frac{\text{Доход от продаж}}{\text{Абсолютные активы}}.$$

В зависимости от величины показателя Z определяется вероятность банкротства предприятия (фирмы): до 1,8 — очень высокая; 1,81-2,7 - высокая, 2,71-3,0 - возможная; более 3 - очень низкая.

Если получено низкое значение Z, то это следует понимать как сигнал опасности, показывающий необходимость более глубокого анализа причин, вызвавших снижение этого показателя экономической безопасности предприятия.

В отечественной практике для оценки устойчивой работы предприятия проводится анализ самоокупаемости производства (определение «точки безубыточности»). Для этого необходимо определить по каждому товару, какие издержки являются постоянными (не зависят от объема производства), а какие — переменными (пропорциональны объему производства). После этого, используя простую формулу, можно подсчитать минимальный объем данного товара, обеспечивающий безубыточность производства:

$$\text{Объем товара, обеспечивающий безубыточность} = \frac{\text{Постоянные издержки}}{\text{Продажная цена} - \dfrac{\text{Переменные издержки}}{\text{Объем реализованных товаров}}}$$

Если спрос на данный товар меньше, чем объем товара, обеспечивающий безубыточность, то его производство не будет самоокупаемым, т.е. вне поля экономической безопасности (рисунок 3). Зарубежные специалисты аналогом этому показателю считают малоизвестную у нас «маржу безопасности» (по методике анализа «breakeven"). По принятому определению, «... это разница (абсолютная или в процентах) между фактическим (расчетным) и минимальным объемом реализации (производства) продукции, ниже которого производство будет невыгодным (убыточным) вследствие высокой доли фиксированных расходов». Экономический смысл «маржи безопасности» заключается в определении того прогнозируемого объема выпуска (продаж), начиная с которого предприятие перемещается в зону экономической безопасности своей деятельности.

Важными для принятия решений, особенно по ценам, являются принципиальные различия подходов в отношении систем счета издержек. Если производится калькуляция издержек в полном объеме, то пытаются охватить все возникающие в связи с общим производством издержки и распределить их по выпущенным изделиям, в крайнем случае путем оценки и разбивки. При калькуляции издержек в частичном объеме признают только издержки, обусловленные непосредственно выпускаемым

изделием и непосредственно относимые к данному изделию, т.е. без постоянных и общих (накладных) издержек, рассматривая их как «издержки производственной готовности», которые хотя и обусловлены намерением предприятия выпускать продукцию, но не вызваны изготовлением отдельного товара.

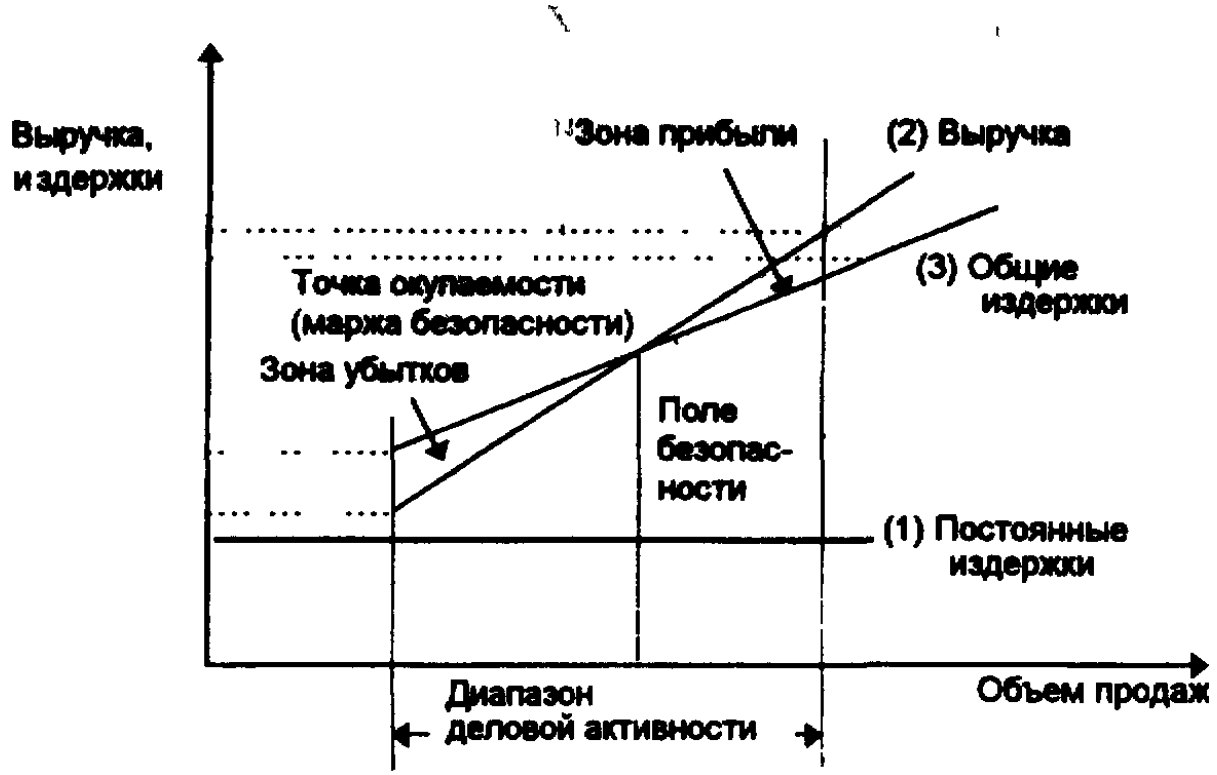


Рисунок 3. Графическое определение маржи и поля экономической безопасности

Так производитель может определить свой нижний предел цен — самую низкую приемлемую цену. С этим нижним пределом цены покрываются переменные издержки или предельные издержки, т.е. издержки, обусловленные непосредственно производством изделия. Любая достигнутая цена выше этого нижнего предела вносит свой вклад в покрытие постоянных издержек (она дает так называемую «долю покрытия»). В зависимости от гибкости спроса вполне может оказаться целесообразным стремиться к увеличению объема реализации путем снижения цены ниже рассчитанного полного объема издержек, так, чтобы постоянные издержки распределялись на большее количество штук и таким образом достигалось бы покрытие полного объема издержек. Даже если это не получается, то цена, не покрывающая полного объема издержек, но превышающая переменные издержки, останется единственно рациональной альтернативой. Возникающие постоянные издержки производитель в короткий срок все равно не может изменить. Поэтому предприятие может стремиться только к тому, чтобы как можно большую часть издержек покрыть за счет продолжительной стабильной продажи изделия. Таким образом, его стратегия будет заключаться в том, чтобы вернуть как минимум переменные издержки (нижний предел цены), но запрашивать при этом максимально достижимую в условиях конкуренции цену. Здесь частичная калькуляция издержек служит как вспомогательный инструмент для принятия решений.

Частичная калькуляция позволяет сделать выводы не о прибыльности отдельного носителя издержек, а только о прибыли в целом за определенный период. Она не дает

также исходных сведений при внедрении на рынке новых изделий или при калькуляции цен в рамках штучного производства, поскольку она указывает только нижний предел цены, но не содержит информации об установлении цен в общем. В принципе предпосылкой является наличие рыночных цен, на которые частичная калькуляция ориентируется в том смысле, что по ним подсчитывают доли покрытия (как разницу между чистой выручкой и переменными издержками). Поэтому при калькуляции исходят не из отдельных издержек благодаря подсчитанной себестоимости, а из рыночных цен и достигнутой или достижимой выручки, с тем чтобы затем после учета издержек рассчитать сумму покрытия и результат предприятия в виде чистого дохода.

Важным показателем для принятия решений на предприятии (фирме) является так называемый «коэффициент покрытия». Он рассчитывается по формуле

$$\text{Коэффициент покрытия} = \frac{\text{Доля покрытия}}{\text{Чистая выручка}}$$

Чем выше коэффициент покрытия, тем больший вклад вносит изделие в покрытие постоянных издержек. Если предприятие (фирма) располагает свободой в принятии решения, то ему следует форсировать изделия с наибольшим коэффициентом покрытия в отношении производства и сбыта.

Расчет цены предложения на рынке можно тоже определить в рамках частичной калькуляции издержек;

$$\text{Цена предложения} = \frac{\text{Переменные издержки на единицу изделияия}}{1 - \text{коэффициент покрытия}}$$

В реальной практике предприятий (фирм) чаще всего существуют общие издержки, которые следует относить не к отдельному изделию, а к определенной группе изделий или подразделению предприятия (фирмы). Точности счета издержек способствует то, что такие издержки относят к причинившему их подразделению, а не просто рассматривают как общие расходы.

4.4. Финансовая диагностика экономической безопасности предприятия

В современных условиях процесс успешного функционирования и экономического развития отечественных предприятий во многом зависит от степени обеспечения их экономической безопасности.

Необходимость постоянного соблюдения экономической безопасности предопределяется для каждого субъекта хозяйствования задачей обеспечения стабильности функционирования и достижения главных целей своей деятельности. Уровень экономической безопасности предприятия зависит от того, насколько эффективно его руководство и специалисты будут способные избежать возможных

угроз и ликвидировать вредные последствия отдельных отрицательных составляющих внешней и внутренней среды.

Главная цель экономической безопасности предприятия состоит в том, чтобы гарантировать его стабильное и максимально эффективное функционирования в данном периоде и высокий потенциал развития в будущем.

К основным функциональным целям экономической безопасности относятся:

✓ обеспечение высокой финансовой эффективности работы, финансовой стойкости и независимости предприятия;

✓ обеспечение технологической независимости и достижения высокой конкурентоспособности технического потенциала предприятия;

✓ достижение высокой эффективности менеджмента, оптимальной и эффективной организационной структуры управления предприятием;

✓ достижение высокого уровня квалификации персонала и его интеллектуального потенциала;

✓ минимизация разрушительного влияния результатов производственно-хозяйственной деятельности на состояние окружающей среды;

✓ правовая защищенность всех аспектов деятельности предприятия;

✓ обеспечение защиты информации, коммерческой тайны и достижения необходимого уровня информационного обеспечения работы всех подразделов предприятия;

✓ эффективная организация безопасности персонала предприятия, его капитала и имущества, а также коммерческих интересов.

Среди функциональных уровней экономической безопасности финансовый считается ведущим и решающим, поскольку в рыночных условиях хозяйствования финансы являются «двигателем» любой экономической системы.

Процесс охраны финансового уровня экономической безопасности следующий:

- анализ угрозы отрицательных действий относительно политико-правовой экономической безопасности;

- оценка текущего состояния финансового уровня экономической безопасности;

- оценка эффективности предотвращения возможного вреда от отрицательных действий относительно финансового уровня экономической безопасности;

- планирование комплекса мероприятий по обеспечению финансового уровня экономической безопасности и разработка рекомендаций относительно его реализации;

- бюджетное планирование практической реализации предлагаемого комплекса мероприятий;

- планирование корпоративных ресурсов;

- оперативная реализация запланированных действий в процессе осуществления предприятием финансово-хозяйственной деятельности.

В процессе оценки текущего состояния финансового уровня экономической безопасности подлежат анализу:

✓ финансовая отчетность и результаты работы предприятия - платежеспособность, финансовая независимость, структура и использование капитала и прибыли;

✓ конкурентное состояние предприятия на рынке - частица рынка, которым владеет субъект хозяйствования; уровень применяемых технологий и менеджмента;

✓ рынок ценных бумаг предприятия - операторы и инвесторы ценных бумаг, курс акций.

Диагностика угроз экономической безопасности предполагает определение и мониторинг факторов, определяющих устойчивость финансово-экономического положения на краткосрочную и среднесрочную перспективу, а также показателей (индикаторов) оценки уровня экономической безопасности; определение их пороговых значений.

От правильного выбора измерителей проявления угроз или системы показателей для мониторинга (то есть индикаторов) зависит адекватность оценки экономической безопасности предприятия. Критические значения индикаторов представляют собой количественные параметры, очерчивающие границу между безопасной и опасной зонами в различных направлениях деятельности предприятия. Диагностика уровня экономической безопасности по системе показателей в необходимых случаях должна учитывать специфические отраслевые особенности предприятий, а пороговые значения показателей следует определять с учетом периодов развития экономики. Система оценочных показателей должна включать не только показатели-критерии, но и дополнительные аналитические показатели, формирующие целостное представление о состоянии хозяйствующего субъекта.

Экономическую безопасность как комплексное понятие следует характеризовать интегральным показателем или интегральной оценкой, рассчитанной на базе частных оценочных показателей.

Рассматривая методы построения такого показателя необходимо учесть ряд аспектов:

✓ в состав индикаторов, определяющих уровень комплексной оценки, в первую очередь следует включать те показатели, которые характеризуют различные стороны финансового состояния предприятия и позволяют оценить его финансовые результаты по различным направлениям;

✓ возможность количественной оценки частных показателей и анализ их взаимосвязи. Изолированное рассмотрение индикаторов не позволяет обоснованно определять их пороговые значения;

✓ при отборе показателей необходимо предусматривать возможность расчета их прогнозных величин;

✓ прогнозирование уровней показателей должно предполагать оценку надежности в зависимости от рассматриваемого временного интервала;

✓ методика расчета комплексного показателя, характеризующего финансовый уровень экономической безопасности предприятия, должна быть достаточно простой и доступной, базирующейся на учетных данных.

ГЛАВА 5
ОСОБЕННОСТИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ РАЗЛИЧНЫХ ОТРАСЛЕЙ

Среди существующих **средств** обеспечения безопасности можно выделить следующие:

1) **Технические средства**. К ним относятся охранно-пожарные системы, видео-радиоаппаратура, средства обнаружения взрывных устройств, бронежилеты, заграждения и т.д.;

2) **Организационные средства**. Создание специализированных оргструктурных формирований, обеспечивающих безопасность предприятия;

3) **Информационные средства**. Прежде всего, это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Кроме этого, важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах;

4) **Финансовые средства**. Совершенно очевидно, что без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей;

5) **Правовые средства**. Здесь имеется в виду использование не только изданных вышестоящими органами власти законов и подзаконных актов, но также разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности;

6) **Кадровые средства**. Имеется в виду, прежде всего, достаточность кадров, занимающихся вопросами обеспечения безопасности. Одновременно с этим решают задачи повышения их профессионального мастерства в этой сфере деятельности;

7) **Интеллектуальные средства**. Привлечение к работе высококлассных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

Следует заметить, что применение каждого из вышеуказанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе. В то же время необходимо отметить, что одновременное внедрение всех вышеуказанных средств в принципе невозможно. Оно проходит обычно ряд этапов:

I этап. Выделение финансовых средств.

II этап. Формирование кадровых и организационных средств.

III этап. Разработка системы правовых средств.

IV этап. Привлечение технических, информационных и интеллектуальных средств.

Переведенные из статичного в динамичное состояние вышеуказанные средства становятся **методами**, т.е. приемами, способами действия. Соответственно, можно говорить о технических, организационных, информационных, финансовых, правовых, кадровых и интеллектуальных методах.

Приведем краткий конкретный перечень этих **методов**:

Технические – наблюдение, контроль, идентификация и т.д.;

Организационные - создание зон безопасности, режим, расследование, посты, патрули и т.д.;

Информационные – составление детективами характеристик на сотрудников, аналитические материалы и учеты конфиденциального характера и т.д.;

Финансовые – материальное стимулирование сотрудников, имеющих достижения в обеспечении безопасности, денежное поощрение информаторов и т.д.;

Правовые – судебная защита законных прав и интересов, содействие правоохранительным органам и т.д.;

Кадровые – подбор, расстановка и обучение кадров, обеспечивающих безопасность предприятия, их воспитание и т.д.;

Интеллектуальные – патентование, ноу-хау и т.д.

5.1. Промышленные предприятия

Проблемы собственной экономической безопасности возникают перед каждым предприятием не только в кризисные периоды, но и при работе в стабильной экономической среде, комплекс решаемых при этом целевых задач имеет существенное различие.

1) В режиме устойчивого функционирования предприятие при решении задач своей экономической безопасности акцентирует главное внимание на поддержании нормального ритма производства и сбыта продукции, на предотвращении материального и/или финансового ущерба, на недопущении несанкционированного доступа к служебной информации и разрушения компьютерных баз данных, на противодействии недобросовестной конкуренции и криминальным проявлениям.

Производственная сфера эффективно работающего предприятия, если она своевременно подвергается необходимой модернизации, не является источником экономического неблагополучия (экономической опасности) как для коллектива предприятия и его собственника, так и для тех агентов рынка, которые пользуются продукцией предприятия, то есть его смежников и потребителей.

2) В кризисные периоды развития наибольшую опасность для предприятия представляет разрушение его потенциала (производственного, технологического, научно-технического и кадрового), как главного фактора жизнедеятельности предприятия, его возможностей. При этом условия хозяйствования таковы, что не

обеспечивается способность потенциала к воспроизводству. Ресурсы для этого предприятие может приобретать только исходя из результатов своей деятельности (точнее — амортизационных отчислений и прибыли), а также за счёт заёмных средств. Оба эти источника инвестиций в кризисной ситуации у предприятия, как правило, оказываются перекрыты.

В настоящее время большинство российских промышленных предприятий, работая в нестабильной экономической среде, является убыточными, переживает глубокий спад производства и находится в критическом или банкротном состоянии. Причин депрессивного развития много, но главные из них кроются в инерции сложившейся структуры производства, его технологической отсталости и физическом износе основных фондов, в отсутствии приоритетов государственной научно-промышленной политики, определение которых позволило бы провести необходимую реструктуризацию мощностей, в условиях хозяйствования, сложившихся в результате неэффективных, с точки зрения реального сектора экономики, преобразований, не позволяющих предприятиям зарабатывать средства на модернизацию.

Такое их положение представляет определенную опасность как для экономики и социальной стабильности в регионе и обществе в целом, так и для потенциала и коллектива каждого конкретного предприятия. Ведь промышленное предприятие, являясь основным структурообразующим элементом экономики, выполняет не только производственную функцию, но и даёт средства к существованию многих людей, связанных с ним, то есть несёт определённую социальную нагрузку и ответственность.

Неполная загрузка мощностей, а потому и неэффективное их использование, а тем более разрушение созданного потенциала предприятия представляют угрозу экономическим, материальным основам жизнедеятельности коллектива и общества, для поддержания которых он создавался и развивался.

Ни одно предприятие не может ощущать себя в экономической безопасности, если его продукция не востребована рынком; ни одно предприятие, производящее средства производства, не может ощущать себя в безопасности, если происходит длительный спад в технологическом развитии страны.

Сейчас наблюдается чётко выраженная тенденция утраты промышленными предприятиями способности производства сложной и наукоемкой продукции, причём не только новой, но и выпускавшейся ими ранее в условиях стабильного развития экономики. Это означает, что под угрозой находится техническое перевооружение производственного аппарата таких базовых отраслей экономики, как энергетика, транспорт, металлургия, химия, добыча полезных ископаемых и т.д., так как по мере износа активной части основного капитала этих отраслей их полноценное замещение новым отечественным оборудованием будет затруднено или невозможно (ведь промышленность более чем на 80% укомплектована машинами и оборудованием именно отечественного производства. Их замена массовыми импортными закупками с финансовой точки зрения вряд ли осуществима).

Многие предприятия этих отраслей просто остановятся, потому что их сложное оборудование (например, в энергетике) имеет, во-первых, длительный цикл изготовления и, во-вторых, не будет достаточных производственных мощностей, чтобы возместить обвальное выбытие основных производственных фондов.

Главный комплекс проблем и основные причины текущего неблагополучия многих промышленных предприятий кроются в:

- невостребованности продукции на внутреннем и внешнем рынках, в её низкой конкурентоспособности;

- истощении инвестиционных ресурсов, усиленном финансовым кризисом, инфляцией, разрушением денежного обращения, издержками действующей системы налогообложения товаропроизводителей;

- невыполнении государством своих обязательств по оплате заказов для своих нужд;

- неэффективных способах институциональных преобразований, повлекших за собой фрагментацию многих некогда единых производственных комплексов на более мелкие, обособление последних и, как следствие, рост транзакционных издержек на каждом переделе не менее чем на 20% и соответствующее удорожание продукции;

- таможенных и валютных барьерах на границах стран СНГ, разрушивших их некогда единое экономическое пространство, и др.

5.2. Интернет и информационные системы

Интернет это одно из самых быстро развивающихся средств коммуникации и, вероятно, наиболее быстро распространяю.

Информация - постоянно обновляемые теоретические знания и различного рода сведения, в том числе практические навыки людей. По мнению специалистов, информация - новый ресурс, единственный продукт не убывающий, а растущий со временем. Чем больше и быстрее внедряется качественной информации в народное хозяйство и специальные приложения, тем выше жизненный уровень народа, экономический, оборонный и политический потенциал страны. Глобальная сеть Интернет инициирует процесс создания новой электронной, виртуальной среды обитания человеческой цивилизации. Совокупное воздействие информационной технологии, Интернет и электронной торговли может вызвать такой же преобразовательный эффект, какой вызвала промышленная революция. Они будут и далее изменять мировой экономический ландшафт и трансформировать организационные структуры государств.

Очевидно, что целостность современного мира как сообщества обеспечивается в основном за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. Уже сегодня, по заявлениям некоторых иностранных экспертов, отключение компьютерных систем приведет к разорению 20% средних компаний в течение нескольких часов, 48% потерпят крах в течение нескольких суток. Около 33% банков будут разорены спустя несколько часов после такой катастрофы, а 50% из них разорятся спустя несколько суток. Сегодня Интернет - это динамическая, в значительной степени самоорганизующаяся система, позволяющая говорить о новом социальном явлении в открытом Internet-сообществе.

В поле зрения хакеров оказались денежная и секретная информация, аппаратура контроля над космическими приборами, ядерными электростанциями, военным комплексом. Успешная атака на такие компьютеры может заменить армию. Оружие "кибертеррористов" постоянно совершенствуется в зависимости от средств защиты, применяемых пользователями компьютерных сетей. Внешние атаки могут преследовать и более серьезные цели, чем пассивный сбор данных, - такие, как, например, выведение из строя главных компьютерных узлов. По мнению экспертов, чтобы парализовать жизненно важные точки созданной инфраструктуры, достаточно нанести удар всего по нескольким десяткам объектов. Одним из первых примеров террористического акта нового поколения в сфере бизнеса является взрыв кустарного электронного фугаса в подземном гараже международного бизнес-центра в Нью-Йорке, осуществленный в середине 1990-х годов. При этом совершенно не пострадали люди и технические средства офисов, а основной ущерб определялся потерей содержания баз данных - программного обеспечения (часто уникального) и собственно хранимой информации.

Примером масштабной и одновременно бессмысленной Интернет-атаки является террористическая акция, осуществленная 7-9 января 2000 года, когда сайты девяти ведущих торговых Интернет компаний подверглись массированному нападению преступников. Утром на главный сайт компании Yahoo поступил почти миллиард обращений. Компьютеры оказались не в состоянии справиться с таким количеством информации (число обращений обычно не превышает 200 млн. в день) и стали выключаться один за другим. Через полчаса сайт Yahoo отключился от сети. Точно таким же атакам подверглись сайты других крупнейших торговых и информационных компаний.

Никаких новых ключей после нападения никто не публиковал. Их просто не было. Во всех атаках использовался алгоритм, опубликованный еще в 1999 году немецким хакером по прозвищу Mixter. Схема атаки проста: компьютеры (в этом случае их было около 100), запрограммированные хакером, посылают на сайт-жертву запросы, ничем не отличающиеся от обыкновенных пользовательских, только делают это с огромной частотой. Компьютеры сайта оказываются не в состоянии обрабатывать такое количество запросов и либо выключаются, либо просто сгорают. Особенность такой атаки в том, что ЭВМ не в состоянии отличить ложные запросы от подлинных. Общий объем потерь от этой акции составил $ 1,2 млрд.

Рост деструктивного потенциала методов современного терроризма призван не только увеличить их материальное поражающее воздействие, но и усилить устрашающее влияние на объекты террористических акций. В значительной мере это достигается террористическими организациями посредством все более активного осуществления информационно-пропагандистской деятельности на основе использования собственно пропагандистского аппарата, независимых средств массовой информации, системы Интернет. Здесь используется путь широкого распространения информации и дезинформации о разрушительных последствиях совершенных террористических акций, об угрозах дальнейшего систематического осуществления актов терроризма, о повышения их разрушительного действия, применении новых террористических средств, нанесении террористических ударов по особо важным для жизнедеятельности общества и безопасности населения объектам с целью запугивания (в соответствии с конкретными стратегическими и тактическими задачами террористов) населения или отдельных его групп, деморализации личного состава

правоохранительных органов, должностных лиц государственного аппарата, устрашения конкретных политических противников. По своим масштабам и действенности информационно-пропагандистские акции террористических организаций (как составляющая общего механизма устрашения террористами объектов их преступной деятельности) играют в настоящее время все большую роль в общей структуре террористической деятельности, что обуславливает необходимость создания эффективной системы антитеррористической контрпропаганды.

Отличительной чертой информационного терроризма является его дешевизна и сложность обнаружения. Система Интернет, связавшая компьютерные сети по всей планете, изменила правила, касающиеся современного оружия. Анонимность, обеспечиваемая Интернетом, позволяет террористу стать невидимым и, как следствие, практически неуязвимым и ничем (в первую очередь жизнью) не рискующим при проведении преступной акции. Положение усугубляется тем, что преступления в информационной сфере, в число которых входит и кибертерроризм, влекут за собой наказание существенно меньше, чем за осуществление "традиционных" террористических актов. В соответствии с Уголовным кодексом Российской Федерации (ст. 273), создание программ для ЭВМ или внесение изменений в существующие программы, которые заведомо приводят к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, наказывается лишением свободы на срок максимум до семи лет. Для сравнения, в США законы карают несанкционированное проникновение в компьютерные сети сроком до 20 лет.

В Российском отделении Всемирного общества "Врачи за права человека" исследовали воздействие на зрителей телевизионных передач. Оказалось, что после негативной информации (которая преобладает а экране) у них резко падают все жизненно важные показатели. Негативные передачи и публикации разрушают жизненные стереотипы. Под воздействием негативной информации кажется, что страт погибла, честных людей не стало, кругом одна жулики. Рушится вера в добро и справедливость, исчезает смысл и радость жизни. Подрываются базовые стереотипы, исчезает психологическая опора. А когда ее нет, резко падает биологическая сопротивляемость организма. Прежде всего, страдает иммунитет – человека.

Снижается жизненный тонус, люди раньше стареют и умирают. Действительно, качество информации и ее доступность, современные информационные технологии, радикально увеличивая объем и скорость распространения информации, вызывают глубокие изменения в политике конкретного государства, оказывая существенное воздействие на характер и системы властвования Точная информация повышает эффективность власти, позволяет вовремя скорректировать избранное направление действий, отреагировать на вновь появившиеся обстоятельства. Вместе с тем и политические структуры воздействуют на информацию, степень ее открытости, процессы распространения, характер передачи потребителю.

Одна из важнейших социальных функций власти -дозирование информации и ее психологическая "упаковка". На этом основывается механизм манипулирования общественным мнением. Самой известной и простой формой властного контроля над информационными процессами выступает цензурная деятельность, в процессе которой государство с помощью специально назначенных и ответственных перед ним

чиновников "управляет" содержанием информационных материалов. Действенным средством регуляции отношений между властью и информацией служит право, сдерживающее произвол как с одной, так и с другой стороны, предполагающее наличие для них взаимных стимулов и ограничений.

Практика показывает, что юридический способ регуляции такого рода отношений наиболее эффективен и приемлем для большинства членов общества. Он в меньшей степени подвержен искажению в ходе функционирования, его элементы общеизвестны и исключают произвольные установления. Кроме того, принятие самих правовых норм происходит в обстановке, как правило, открытого обсуждения.

Между тем информатизация современной России, насыщение ее новыми технологиями происходят при недостаточном нормативно-правовом обеспечении. Принято несколько нормативно-правовых актов: Доктрина информационной безопасности Российской Федерации от 28.09.2000, федеральные законы "Об электронной цифровой подписи" от 10.01.2002, "Об информации, информатизации и защите информации" от 20.01.1995, "Об участи в международном информационном обмене" от 4.07.1996 и другие. Несмотря на определенное внимание государства в настоящее время к правовому обеспечению информационного процесса, тем не менее, состояние нормативно правовой базы требует совершенствования. Для сравнения, сфера информационных технологий США регламентируется более чем 300 специальными законами и подзаконными актами . Одной из важнейших проблем на пути создания информационного общества в России являются формирование и развитие его правового фундамента, основу которого составляет специальное информационное законодательство. Эта новая отрасль российского законодательства призвана обеспечить регулирование отношений в информационной сфере при создании, движении и потреблении информации в обществе. США, Германия, Франция и другие страны гораздо раньше приступили к формированию такого законодательства.

Их опыт позволяет выявить следующие направления, которые необходимо учитывать в российской практике:

а) развитие и применение институтов авторского и патентного права, регулирующих отношения при создании информации разного вида и назначения;

б) регламентация отношений, возникающих при создании информационных ресурсов, при подготовке и предоставлении информационных услуг;

в) создание условий для развития и применения информационных систем, информационных технологий и средств их обеспечения;

г) гарантирование информационной безопасности;

д) установление и реализация права юридических и физических лиц на информацию.

Формирование и развитие российского информационного законодательства - широкомасштабная деятельность, проникающая во все отрасли права, охватывающая правотворчество различных органов государства, предполагающая в этом процессе разных субъектов. Такую деятельность, по мнению специалистов, необходимо проводить по специальной федеральной программе, в рамках осуществления определенной информационно-правовой политики. Одним их важнейших

результатов данной политики должно стать создание Информационного кодекса Российской Федерации, а, в конечном счете - формирование высокой информационно-правовой культуры должностных лиц и граждан1.

Особо следует отметить усилия нашей страны в плане борьбы с информационным терроризмом на международной арене. В частности, Россия предложила на рассмотрение ООН пакет международных принципов, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем и на борьбу с информационным терроризмом и криминалом.

В документе зафиксировано право каждого как на получение и распространение информации, так и на защиту своих информационных ресурсов от неправомерного использования и несанкционированного вмешательства. Особое внимание обращается на необходимость принятия мер для ограничения угроз в сфере международной информации. В частности, взять на себя обязательства по отказу от действий по нанесению ущерба другим государствам в области информации, по доминированию и контролю в информационном пространстве, по поощрению действий террористических и преступных сообществ, по организации информационных воин, по манипулированию информационными потоками и по информационной экспансии.

Таким образом, проблемы информационного терроризма затрагивают сегодня каждого, кто имеет дело; информационными технологиями. Мировые тенденции таковы, что рано, или поздно, информационный терроризм будет нацелен на мировую экономику.

Методы информационного терроризма совершенно иные, чем в традиционном: не физическое уничтожение людей (или его угроза) и ликвидация материальных ценностей, не разрушение важных стратегических и экономических объектов, а широкомасштабное нарушение работы финансовых и коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и навязывание властным структурам своей воли.

Основой обеспечения эффективной борьбы с кибертерроризмом является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению такого рода деятельности. Для борьбы с терроризмом во всех его проявлениях работают различные антитеррористические органы.

Особое внимание борьбе с терроризмом уделяют развитые страны мира, считая его едва ли не главной опасностью для соседства. И это обосновано. Так как информационный терроризм как современное социально-политическое влияние представляет серьезную угрозу безопасности и жизненно важным интересам, как личности, так и правительства и государства. Но полностью обезопасить общество от террористов невозможно, можно лишь снизить угрозу превентивным контролем и борьбой с непосредственными исполнителями террористических актов.

5.3. Строительство

Строительная отрасль - одна из наиболее существенных и развивающихся отраслей экономики России. По темпам строительства можно судить о состоянии экономики в целом.

Нормальное функционирование предприятий и организаций в современных условиях требует все большего искусства в управлении. В настоящее время в ряде монографических работ, изданий, учебных пособий, методических рекомендаций, диссертаций очень детально рассмотрены такие темы, как система управления предприятия, организационная структура предприятия, контроллинг, управленческий учет, бухгалтерский учет, документооборот, аудит, внутренний контроль, кадровая политика, риск-менеджмент и другие темы. Однако в большинстве случаев они рассматриваются без учета необходимости обеспечения экономической безопасности всего сложного комплекса, каким является современное предприятие. Опыт автора говорит о том, что на практике специалистам в соответствующих областях приходится так или иначе сталкиваться с проблемой обеспечения экономической безопасности.

Анализ ряда ситуаций из практики приводит к следующему выводу: во всех рассмотренных случаях нанесения экономического ущерба строительному предприятию использовались существующие, либо специально создавались недостатки его устава, организационной структуры, построения бизнес-процессов, использовались личностные и профессиональные качества учредителей и руководителей. При этом в большинстве случаев проведение процедур контроля, аудиторских и прочих проверок, а также «традиционных» мероприятий службы безопасности не смогло обеспечить экономическую безопасность предприятия. Также нашумевшие за последнее время скандалы с гигантами западной индустрии, такими как Enron, Par-malat, Worldcom, говорят о недостаточной эффективности ставших традиционными мероприятий. Следовательно, необходимы иные подходы к проблеме экономической безопасности строительного предприятия. При этом очень важно, чтобы вопросы обеспечения экономической безопасности принимались во внимание, начиная с момента учреждения предприятия, формирования органов управления, определения организационной структуры и построения бизнес-процессов. Большое внимание стоит уделять взаимодействию подразделений предприятия со службой безопасности, так как оно сильно влияет на эффективность и стоимость мероприятий по обеспечению экономической безопасности предприятия.

Экономическая безопасность строительного предприятия - это свойство предприятия, характеризуемое его способностью нормально функционировать для достижения своих целей при существующих внешних условиях и их изменении в определенных пределах. Под нормальным мы понимаем такое функционирование предприятия, которое в существующих внешних условиях обеспечивает достижение им поставленных целей оптимальным образом или достаточно близким к нему.

Механизм реализации комплексного подхода к решению проблем обеспечения экономической безопасности строительного предприятия состоит в организации единого комплекса мер, обеспечивающих безопасность предприятия. Он рассматривает всю финансово-хозяйственную деятельность предприятия, а не только систему безопасности в узком смысле. Необходимо не разрабатывать и проводить

комплекс мероприятий по защите созданного предприятия и его существующей текущей деятельности, а сразу создавать предприятие, организовывать и вести деятельность, предусматривая их устойчивость к угрозам как обязательное свойство. Также целесообразно рассмотреть возможность расширения сферы влияния службы безопасности на всю деятельность предприятия, углубление степени влияния службы безопасности, улучшение ее взаимодействия с подразделениями предприятия и внешней средой, внедрение новых способов деятельности.

5.4. Торговля

5.4.1. Оптовая торговля

Торговля как вид деятельности имеет свои характерные особенности. В торговле как в отрасли товарно-материальные ценности в цикле «товар - деньги - товар» претерпевают, пожалуй, наименьшие изменения. Возможные изменения - это фасовка, придание товарного вида, предпродажная подготовка. Прежде всего стоит отметить, что торговля бывает двух видов - оптовая и розничная.

Покупателями для предприятий оптовой торговли, как правило, выступают (мелко)оптовые предприятия торговли, предприятия розничной торговли, предприятия других отраслей экономики. Товар отгружается относительно крупными партиями, Доставка товара может осуществляться как силами покупателя, так и силами продавца или силами третьей стороны по договору с продавцом или покупателем.

Для хранения, затаривания, отгрузки товара обычно используется склад. Склад может быть собственный или арендуемый. Также возможны варианты размещения товара на специализированных складах, их использование может быть обусловлено как особенностями финансово-хозяйственной деятельности, так и требованиями законодательства (например, акцизный склад, таможенный склад). Также могут иметь место прямые поставки, при которых товар, минуя склад торговой организации, поступает со склада поставщика непосредственно на склад покупателя.

Производственный цикл оптовых торговых предприятий обычно выглядит следующим образом (при ряде допущений об особенностях финансово-хозяйственной деятельности предприятий торговли):

✓ решение о закупке товара;

✓ заключение договора на поставку товара в адрес торговой организации;

✓ оплата товара продавцу;

✓ отгрузка продавцом товара;

✓ доставка товара от склада продавца (производителя) на склад предприятия;

✓ разгрузка товара и его приемка, составление актов приема-передачи;

✓ оприходование товара;

✓ размещение товара на складе и его хранение;

✓ принятие решения о продаже товара;

✓ заключение договора на поставку товара торговой организацией покупателю;

✓ получение предоплаты;

✓ отгрузка товара и его списание;

✓ доставка товара покупателю;

✓ разгрузка товара покупателем и его приемка, подписание накладных или составление актов приема-передачи.

На каждой из этих фаз может наноситься ущерб предприятию и, соответственно, существуют угрозы экономической безопасности.

Укажем некоторые из критериев нормальности для двух первых этапов вышеприведенной последовательности, предоставив читателю возможность провести аналогичную работу в полном объеме и для остальных этапов.

Решение о закупке товара можно считать правильным, если товар закупается по цене не выше рыночной и может быть перепродан с выгодой в течение разумного времени в количестве, соответствующем закупке.

Соответствующие угрозы:

✓ товар закупается в большем или меньшем количестве, чем необходимо;

✓ товар закупается по цене более высокой, чем рыночная цена.

Договор на поставку можно считать нормальным, если его существенные условия соответствуют технологии работы торгового предприятия и соответствуют сложившимся обычаям хозяйственной деятельности. Для торговых предприятий можно отметить следующие существенные условия:

1. Сроки поставки. Вообще, срок поставки для договора поставки с юридической точки зрения является существенным условием. Без его указания заключенный договор вообще не является договором поставки. Кроме того, сроки поставки должны обеспечивать торговому предприятию возможность планировать свою деятельность и эффективно управлять запасами. Предусмотренные договором отклонения в сроках поставки должны быть таковы, чтобы не сказываться на бесперебойном обеспечении торгового предприятия товаром. Соответственно договором должны быть предусмотрены эффективные санкции за срыв сроков поставки.

2. Способ доставки товара. Транспортные издержки, разгрузочно-погрузочные расходы составляют весьма существенную часть себестоимости получаемого товара. Кроме того, при доставке товара могут происходить хищения части товара, его порча. При перегрузках может также возникать пересортица. Выбор способа доставки - серьезная логистическая задача, и от ее решения может зависеть выгодность торговли данным товаром вообще.

3. Момент перехода права собственности (и соответственно рисков) на товар.

Соответственно любое возможное нарушение критериев нормальности должно рассматриваться как угроза экономической безопасности торгового предприятия.

5.4.2. Розничная торговля

С точки зрения экономической безопасности в части закупок товара предприятие розничной торговли практически ничем не отличается от предприятий оптовой торговли.

В зависимости от организации продажи товара предприятия розничной торговли можно разбить на несколько категорий. Впрочем, деление это довольно условное и не претендует на полноту:

✓ магазины самообслуживания (гипермаркеты, супермаркеты, универсамы);

✓ магазины с «классическими» витринами и продавцами. Рассмотрим критерии «нормальной» работы торгового зала универсама.

При этом контроль качества товара, сроков его реализации отнесем к вопросам управления, а не безопасности. Будем считать, что продажа идет нормально, если:

✓ весь товар с прилавка проходит через кассу;

✓ весь товар правильно идентифицируется на кассе;

✓ кассир правильно принимает денежные средства за прошедший через кассу товар.

Возможные нарушения:

✓ товар скрыто проносится покупателями при проходе через кассу;

✓ товар скрыто проносится покупателями при проходе через выход «без покупок»;

✓ товар неправильно идентифицируется на кассе;

✓ кассир принимает денежные средства в ненадлежащем количестве, неплатежеспособными или фальшивыми денежными знаками;

✓ кассир, находящийся в сговоре с покупателем, проносит товар мимо сканера без его фактического сканирования.

Рассмотрим данные ситуации подробно. Товар может проноситься скрыто покупателем:

✓ в одежде и под одеждой;

✓ в сумке, ранце, портфеле;

✓ в товаре;

✓ товар также может быть вывезен, будучи оставленным в тележке для товара.

Методы предупреждения по выносу под одеждой:

✓ визуальный контроль торгового зала с использованием средств видеонаблюдения;

✓ визуальный контроль торгового зала нейтрально одетыми сотрудниками службы безопасности;

✓ визуальный контроль выходящих покупателей кассирами и сотрудниками службы безопасности;

✓ доставка мелких дорогостоящих товаров на кассу сотрудниками предприятия либо реализация такого товара в отдельных кассах на площади торгового зала.

Методы предупреждения по выносу в ручной клади:

✓ визуальный контроль торгового зала с использованием средств видеонаблюдения;

✓ визуальный контроль торгового зала переодетыми сотрудниками службы безопасности;

✓ доставка мелких дорогостоящих товаров на кассу сотрудниками предприятия либо реализация такого товара в отдельных кассах на площади торгового зала сдача сумок, портфелей, рюкзачков и пр. в места хранения;

✓ запечатывание сумок, портфелей, рюкзачков и пр. в пластиковый пакет.

Метод предупреждения по вывозу в тележках:

✓ - визуальный контроль тележек кассирами и сотрудниками службы безопасности.

Для обеспечения контроля могут использоваться зеркала, позволяющие кассиру видеть дно тележки, не вставая с рабочего места.

Товар неправильно идентифицируется на кассе. Возможные варианты:

✓ случайная ошибка маркирования/считывания штрих-кодов;

✓ переклейка покупателем штрих-кодов с одного товара на другой;

✓ замена покупателем штрих-кодированной упаковки с одного товара на другой;

✓ добавление однородного товара в уже штрих-кодированную упаковку.

Методы противодействия:

✓ все виды визуального контроля зала;

✓ контроль кассирами соответствия товара его штрих-кодовой этикетке по номенклатуре и приблизительно либо точно - по количеству.

Кассир, находящийся в сговоре с покупателем, проносит товар мимо сканера без его фактического сканирования либо пропускает товар с неправильными штрих-кодами. При этом внешне вся ситуация выглядит нормально и от обычной «нормальной» продажи неотличима.

Методы противодействия:

✓ визуальный контроль работы кассиров сотрудниками службы безопасности;

✓ организация сверки чеков выходящих покупателей с товаром, приобретенным ими.

Безусловно, внимательность во время работы как кассиров, так и сотрудников службы безопасности требует постоянной проверки и оценки. Одним из наиболее эффективных способов являются тестовые «покупки». Сотрудник службы безопасности, незнакомый кассирам торгового зала, собирает (либо получает готовую от службы безопасности) тележку, в которой имеются товары с переклеенными штрих-кодами, измененной упаковкой, перевесом товара и т.д. После этого он в роли обычного покупателя проходит через кассу.

Рассмотрим отраслевые особенности торговых предприятий.

Территориальный фактор. Для торговли, особенно розничной, фактор местонахождения места сбыта (магазина) играет первоочередную роль. Магазин, расположенный в удачном («проходном») месте, может быть гораздо выгоднее другого аналогичного исключительно в силу месторасположения. Количество удачных для торговли мест ограничено. Соответственно, все моменты, связанные с организацией места торговли, имеют повышенное значение. Следует уделять особое внимание:

✓ отношениям с местными властями;

✓ отношениям с арендодателями в случае аренды торговых площадей;

✓ мониторингу выделения новых площадей, строительства новых торговых объектов, центров, рынков.

Разобщенность объектов. Обычно характерна для сетевых предприятий розничной торговли, оптовых и розничных предприятий в случае территориального разнесения управляющего офиса и склада (магазинов). Порождает следующие угрозы:

✓ падение управляемости процессом поставок и продаж;

✓ рост транспортных рисков;

✓ хищение ТМЦ на складах, при перевозке и в магазинах.

5.4.3. Сезонность продаж

Обусловливает более высокую требовательность к управлению закупками и продажами. Закупка большего количества сезонного товара, чем требуется, может повлечь за собой задержку его реализации почти на год, до следующего сезона. В случае со скоропортящимся товаром ситуация особенно сложная, так как он может просто прийти в негодность. Порождает следующие угрозы:

✓ фактор погодных рисков;

✓ нанесение экономического ущерба вследствие ошибок управления;

✓ также усугубляет проблему персонала: предприятие вынуждено либо содержать большой штат сотрудников с вынужденными простоями в периоды с низкой загрузкой, либо привлекать дополнительных сотрудников в периоды с высокой нагрузкой.

5.5. Транспорт и связь

Для этих отраслей, оказывающих услуги, в целом характерна следующая особенность. При оказании услуг связи (телефон, телеграф), как правило, не происходит никакого существенного физического перемещения или преобразования товарно-материальных ценностей. В результате факт оказания услуг часто не имеет материального подтверждения. При оказании услуг в сфере транспорта (а также услуг традиционной почты) происходит перемещение товарно-материальных ценностей или пассажиров, но спустя некоторое время после транспортировки факт оказания услуг или же их объем также трудно определить.

Поэтому связь и транспорт являются отраслями, близкими по идеологии нанесения ущерба предприятиям данных отраслей экономики и достаточно легким получением выгоды.

На транспорте основными угрозами являются осуществление неучтенных услуг, а также списание товарно-материальных ценностей и иных ресурсов (ГСМ, электроэнергия, ремонт, запчасти) сверх обусловленных производственной необходимостью. В добавление к ним в зависимости от вида транспорта добавляются специфические угрозы. Их описание выходит за рамки нашей книги.

В сфере связи наиболее характерными являются следующие угрозы:

- административные риски;
- оказание неучтенных услуг («неучтенный трафик»).

Административные риски большинство из читателей представляют себе более чем хорошо. Остановимся более подробно на неучтенном трафике. Трафик - это фактически объем оказанных услуг связи. Технологические особенности предприятий отрасли приблизительно следующие.

Информация об оказанной услуге связи (разговоре, переданной информации, сообщении, пр.) накапливается в специальной программе, управляющей средствами связи. Далее эта информация чаще всего передается в другую программу, где происходит учет расчетов с потребителями (биллинг) оказанной услуги. Существуют и другие алгоритмы предоставления услуг связи. Например, перед предоставлением услуги связи программа управления средствами связи может делать запрос - оплачена ли запрашиваемая услуга абонентом или нет. После тарификации информация поступает в базу данных, откуда ее получают бухгалтерия и соответствующие подразделения предприятия связи (клиентский отдел, например).

Идеологически важным здесь является наличие достаточно длинной цепочки передачи и обработки информации, объективно обусловленной технологией процесса предоставления услуг связи. При передаче информации от программы к программе в силу ряда причин могут происходить искажения передаваемой информации.

В случае, если впоследствии невозможно абсолютно достоверно установить для каждого из звеньев этой цепочки входящую и исходящую информацию, то это обстоятельство, вероятно, будет использовано для нанесения ущерба предприятию.

(Пример с предприятием связи был приведен выше.) Для получения выгоды, скорее всего, будет использована структура-посредник. В отрасли связи таким посредником может быть дилер, виртуальный оператор.

5.6. Экономическая безопасность вузов

Понятие экономическая безопасность вузов вкладывается в следующую понятийную схему: безопасность - национальная безопасность - экономическая безопасность - экономическая безопасность в сфере образования - экономическая безопасность системы высшего и послевузовского профессионального образования - экономическая безопасность вузов и научных учреждений. При этом под угрозой понимается совокупность условий, процессов, факторов, препятствующих реализации экономических интересов образовательных учреждений. Угроза экономической безопасности вуза в конечном виде может быть выражена в виде ущерба, характеризующего снижение экономического потенциала вуза.

В приказе Федерального агентства по образованию от 18 ноября 2008 года N 1615 "О состоянии и мерах по укреплению финансово-хозяйственной дисциплины в подведомственных учреждениях Федерального агентства по образованию" отмечается, что, несмотря на проводимую агентством профилактическую, инструктивно-методическую и аналитическую работу, контрольно-ревизионные мероприятия, общее состояние финансово-хозяйственной деятельности в подведомственных образовательных учреждениях медленно меняется к лучшему. В указанном документе отмечаются нарушения законодательства об образовании и нормативно-инструктивных требований, факты нецелевого использования бюджетных средств, несвоевременной выплаты социальной стипендии, нарушения Порядка ведения кассовых операций, несоблюдение правовых требований при сдаче в аренду имущества, отсутствие контроля за своевременных и полным перечислением средств за обучение, оплаты за проживание, арендной платы, оплаты коммунальных услуг. В приказе отмечается об издании по результатам ревизий более тридцати приказов агентства. В большинстве случаев, они касаются деятельности образовательных учреждений среднего профессионального образования. До сведения образовательных учреждений были доведены и ряд приказов о нарушениях, выявленных в образовательных учреждениях высшего профессионального образования.

Часто встречающиеся нарушения финансово-хозяйственной деятельности в вузах - это нарушения, связанные с оформлением прав на имущество и неодополучением дохода от его использования; нарушения, связанные с исполнением бюджета; нарушения в области оплаты труда и выплате стипендий; нарушения при оплате товаров, работ и услуг; нарушения порядка ведения кассовых операций; нарушения в ведении учета и отчетности. Однако, часто встречающиеся и значительные по размеру причиняемого ущерба - это нарушения в области закупок и определения стоимости ремонтно-строительных работ.

Таким образом, основные риски экономической безопасности вузов возникают в области закупок и при определении объемов и стоимости ремонтно-строительных

работ. В этой связи представляется возможным выработать некоторые рекомендации по снижению рисков экономической безопасности вузов, путем совершенствования отдельных контрольных процедур.

Основными этапами процесса закупок являются составление и рассмотрение заявок; размещение заказа; оплата товаров, работ, услуг; оприходование. Следует обратить внимание на то, что этапы могут быть до известной степени детализированы, а также изменять некоторую последовательность. Например, оприходование не всегда может быть завершающим этапом - распространенный сегодня порядок оплаты (предоплата 30 %, окончательная оплата - 70 %) требует разделения этапа оплаты на предварительную до оприходования и окончательную после оприходования и т.д.

Основной задачей обеспечения экономической безопасности в области закупок является выявление рисков, анализ и тестирование контрольных процедур. Выявление рисков следует производить во взаимосвязи с угрозами и факторами, их создающими.

Контрольными процедурами в области закупок могут быть следующие.

На этапе составления заявок следует обращать внимание на следующие аспекты:

а) имеется ли в вузе утвержденный план закупок (программа размещения заказов) и не превышены ли фактические показатели по отношению к плановым;

б) осуществляется ли корректировка планов закупок и программ размещения заказов в связи с возрастающими потребностями вуза;

в) осуществляется ли сравнение плановых показателей с достигнутыми.

На этапе размещения заказов необходимо уделить внимание:

а) соответствует ли процедура размещения заказов установленным требованиям;

б) учтены ли в конкурсной документации все условия по доставке, форме расчетов, оплате, дате поставки и др.

На этапе оплаты необходимо установить:

а) выполнены ли условия контракта;

б) проведена ли сверка кредиторской задолженности;

На этапе оприходования важно:

а) обеспечена ли приемка товаров, работ и услуг;

б) оформлена ли соответствующим образом первичная документация.

Что касается ремонтно-строительных работ, то здесь также можно выделить несколько основных этапов:

Основной задачей обеспечения экономической безопасности в области ремонтно-строительных работ является выявление рисков, анализ и тестирование контрольных процедур.

На этапе сметного планирования следует обращать внимание на следующие аспекты:

а) предваряется ли сметное планирование комиссионным осмотром и составлением дефектных ведомостей;

б) соответствуют ли применяемые единичные расценки требованиям к составлению проектно-сметной документации;

в) соответствуют ли планируемые объемы работ реальной потребности.

На этапе размещения заказов необходимо уделить внимание:

а) соответствует ли процедура размещения заказов установленным требованиям;

б) учтены ли в конкурсной документации все условия по видам работ, форме расчетов, оплате, приемке работ и др.

На этапе технического надзора следует установить:

а) обеспечено ли наблюдение за ходом работ, в особенности скрытых работ;

б) достаточна ли квалификация работников, осуществляющих контроль за ходом работ со стороны заказчика.

На этапе приемки работ важно:

а) обеспечена ли комиссионная приемка работ;

б) оформлена ли соответствующим образом первичная документация.

На этапе оплаты необходимо установить:

а) выполнены ли условия контракта;

б) проведена ли сверка кредиторской задолженности.

Эффективная система обеспечения экономической безопасности вуза должна предполагать тестирование контрольных процедур. Тестирование контрольных процедур представляется возможным проводить по двум направлениям:

- соблюдение разработанных регламентов контрольных процедур;
- отслеживание ошибок в регламентах контрольных процедур.

Таким образом, понимание основных рисков экономической безопасности, природы их возникновения в вузах и на этой основе создание регламентов контрольных процедур позволит руководителям, должностным лицам и работникам вузов избежать фактов нарушений финансово-хозяйственной деятельности, а тем самым обеспечить развитие экономики системы высшего и послевузовского профессионального образования.

ГЛАВА 6
ПОСТРОЕНИЕ СИСТЕМЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

6.1. Общие принципы

Многие авторы при рассмотрении систем безопасности явно или скрыто используют одну и ту же последовательность рассуждений. Первоначально идеологически предполагается наличие предприятия со своей финансово-хозяйственной деятельностью, затем появление угроз предприятию и уже затем ввиду необходимости защиты от угроз создание системы безопасности. Если в системе безопасности задействованы различные методы и средства обеспечения безопасности, то она признается реализацией комплексного подхода. Таким образом, комплексность в понимании многих авторов - это все возможность и разнообразие видов защиты от различных угроз.

Возможен иной механизм реализации комплексного подхода, как уже отмечалось выше. Как единый комплекс, обеспечивающий безопасность предприятия, предлагается рассматривать всю финансово-хозяйственную деятельность предприятия, а не только систему безопасности в узком смысле. То есть предлагается не разрабатывать и проводить [Комплекс мероприятий по защите созданного предприятия и его действующей текущей финансово-хозяйственной деятельности, а сразу организовывать предприятие и вести финансово-хозяйственную деятельность, предусматривая их устойчивость к угрозам как 5язательное свойство. В случае, если предприятие уже создано ведет финансово-хозяйственную деятельность, то для обеспечения экономической безопасности может быть целесообразно изменить устав, организационную структуру, построение бизнес-процессов.

Такой подход:

- предусматривает необходимость учета требований безопасности начиная последовательно с этапа учреждения предприятия, составления устава, найма сотрудников, до разработки организационной структуры, построения бизнес-процессов, написания должностных инструкций, вплоть до ведения текущей финансово-хозяйственной деятельности;
- рассматривает собственную безопасность не как дополнение к предприятию ввиду необходимости, а как его органичную часть, принимающую участие в финансово-хозяйственной деятельности наравне с другими подразделениями;
- по всей видимости, должен снижать общие затраты предприятия на обеспечение экономической безопасности и повышать эффективность работы по обеспечению экономической безопасности (к сожалению, у авторов нет достаточной сравнительной статистики по этому вопросу);

- согласуется с выводами специалистов по развитию предприятий, которые указывают на низкую эффективность автономных контрольных служб и на необходимость в первую очередь построения контрольной службы с разработкой, увязкой и согласованием широкого спектра мероприятий'.

Фактически на практике этот подход реализуется на предприятиях, которые можно условно разбить на две группы. Первая группа - это предприятия, которые в силу специфики своей деятельности явно и постоянно испытывают ряд угроз, и высокий уровень обеспечения экономической безопасности для них очевидно и безусловно необходимое условие деятельности. Вторая группа - это предприятия, на которых собственники или руководство являются в прошлом сотрудниками правоохранительных органов или в силу ряда причин велико влияние служб безопасности,

С учетом вышесказанного построение системы безопасности в соответствии с предложенным механизмом реализации комплексного подхода должно происходить следующим образом;

- такие компоненты системы безопасности, как политика, стратегия и концепция безопасности, разрабатываются с учетом научной теории безопасности одновременно с разработкой основополагающих положений для предприятия (миссия, стратегия, устав, пр.) в целом и не противоречат им;

- в соответствии с ними создается система безопасности, являющаяся ядром системы обеспечения экономической безопасности предприятия. В деятельности системы безопасности существенное внимание уделяется взаимодействию с другими подразделениями предприятия, организации их деятельности таким образом, чтобы наиболее эффективно и гарантированно обеспечить экономическую безопасность предприятия;

- в соответствии с ними вырабатываются и учитываются требования безопасности к оргструктуре и финансово-хозяйственной деятельности предприятия, формируется оргструктура, регламентируется финансово-хозяйственная деятельность предприятия.

Существуют различные классификации принципов построения системы безопасности предприятия:

- законность;
- комплексное использование сил и средств;
- координация и взаимодействие внутри и вне предприятия;
- компетентность;
- экономическая целесообразность;
- плановая основа деятельности;
- системность;
- приоритет мер предупреждения (своевременность);
- непрерывность;

- экономность;
- взаимодействие;
- сочетание гласности и конфиденциальности;
- комплексность;
- эшелонирование;
- надежность;
- разумная достаточность;
- непрерывность.

Безопасность предприятия должна быть:

- непрерывной;
- плановой;
- централизованной;
- активной;
- надежной;
- универсальной;
- комплексной.

6.2. Создание и организационная структура служб безопасности предприятий

Как было отмечено выше, ядром системы безопасности предприятия, его основой является служба безопасности (СБ) предприятия.

В практике российских предприятий, исследованиях и в литературе помимо термина «служба безопасности (СБ) встречаются следующие названия подразделений предприятия, деятельность которых непосредственно связана с обеспечением экономической безопасности предприятия (ЭБП): служба охраны, отдел безопасности, служба экономической безопасности предприятия и пр.

Виды услуг, которые СБ разрешается предоставлять своему предприятию-учредителю (или функции СБ):

- выявление недобросовестной конкуренции со стороны других предприятий;
- сбор сведений по уголовным делам;
- расследование фактов разглашения коммерческой тайны предприятия;
- сбор информации о лицах, заключивших контракт с предприятием;

- поиск утраченного имущества предприятия;
- расследование фактов неправомерного использования товарных (фирменных) знаков предприятия;
- розыск без вести пропавших сотрудников;
- выявление некредитоспособных партнеров;
- выявление ненадежных деловых партнеров;
- сбор сведений по гражданским делам;
- изучение криминальных и негативных аспектов рынка;
- сбор информации для проведения деловых переговоров;
- защита жизни и здоровья персонала от противоправных посягательств;
- охрана имущества предприятия;
- обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и официальных мероприятий;
- консультирование и предоставление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности;
- проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Современные предприятия - как правило, крупные акционерные общества, зачастую входящие в структуры холдингового типа. Таким образом, у такого предприятия есть акционеры (собственники), может быть выборный орган управления (совет директоров) и подотчетный ему руководитель предприятия - генеральный директор.

6.3. Права, обязанности и ответственность сотрудников Службы безопасности

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, **имеют право**:

✓ требовать от всех сотрудников фирмы, партнеров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;

✓ вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности **обязаны**:

✓ осуществлять контроль за соблюдением инструкции по защите коммерческой тайны;

✓ докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действиях, могущих привести к утечке конфиденциальной информации или утрате документов или изделий;

✓ не допускать неправомерного ознакомления с документами и материалами, имеющими гриф «Коммерческая тайна», посторонних лиц.

Сотрудники службы безопасности несут **ответственность** за личное нарушение безопасности коммерческой тайны и за неиспользование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

6.4. Взаимодействие руководства с сотрудниками Службы безопасности

Проинформируйте сотрудников, с какой целью предпринимаются те или иные меры предосторожности. В этом случае не возникнет непонимания и возражений. От сотрудников, понимающих и разделяющих вашу озабоченность по поводу обеспечения безопасности, всегда можно ожидать проявления большей сознательности и помощи.

Проследите за тем, чтобы все сотрудники службы безопасности имели хорошую профессиональную подготовку. Они должны быть способны решать каждодневные проблемы, проявляя вежливость и профессионализм.

Хорошо подготовленный охранник вряд ли поведет себя неадекватно в стрессовой ситуации. Если сотрудники службы безопасности имеют разрешение на ношение и применение какого-либо вида оружия (включая полицейскую дубинку и особенно огнестрельное оружие), убедитесь, что они могут пользоваться ими, и что оружие применяется в полном соответствии с законом. Границы и случаи применения оружия должны быть оговорены и утверждены руководством, юрисконсультом и начальником службы безопасности компании. Помните, что охранник неподготовленный к рукопашному бою может применить в случае опасности оружие. Личный состав службы безопасности должен быть хорошо подготовлен также и для того, чтобы иметь инициативу в критической ситуации.

Сотрудники службы безопасности должны знать все уязвимые места компании и периодически осуществлять оценку возможной угрозы. Хорошо подготовленный охранник также должен знать основы оказания первой медицинской помощи и способы пожаротушения.

Рутина и скука – враги хорошей службы безопасности. Механическая часто повторяющаяся работа притупляет реакцию личного состава службы безопасности и приводит к невнимательности. Оставленные на долгое время на изолированных постах сотрудники службы безопасности утрачивают бдительность и становятся уязвимыми для внезапных нападений. По возможности меняйте их каждодневные обязанности. Устраивайте частые тренировки и учения. Чем их больше, тем лучше, т.к. это не только оттачивает их навыки, но и поддерживает моральный дух. Вы должны чаще проверять их бдительность и реакцию. Не информируйте служащих компании о

запланированной учебной попытке сотрудников службы безопасности прокрасться на ваш завод или в головной офис или же попытайтесь пройти КПП с фальшивым пропуском и под различными предлогами. Припаркуйте подозрительную машину около здания и проследите, как долго она не будет замечена службой охраны, и какие меры они предпримут в этой связи. Проследите, могут ли посторонние люди получить доступ к секретной документации и главному производственному оборудованию.

Дайте почувствовать сотрудникам службы безопасности, что их работа важна. Существует тенденция относиться к сотрудникам службы безопасности как к огнетушителю, запрятанному где-то за стеклянной дверью и необходимому только в крайнем случае. Это не правильно. Сотрудники службы безопасности должны знать, что они являются частью компании, важным элементом производства продукции и услуг, которые вы продаете, и не менее важными, чем инженерно-технический состав, исследователи рыночных условий и юристы.

В любой ситуации не относитесь к сотрудникам службы безопасности, как к носильщикам или просто, как к неквалифицированным рабочим, которым можно поручить любую грязную работу. Если вы не будете к ним относиться как к профессионалам, они также непрофессионально будут действовать в критической ситуации.

Регулярно интересуйтесь мнением сотрудников службы безопасности. Никто не может знать лучше сотрудников службы безопасности, есть ли уязвимые места в системе безопасности вашей компании.

Не подвергайте сотрудников службы безопасности необоснованному риску. Хорошо укрепленная будка и телевизионная камера с замкнутым контуром уменьшат степень уязвимости охранников и позволят им оперативно и четко отреагировать на внезапное нападение или на другую опасность. Более того, охранники, несущие службу на внешних постах, у ворот или других стратегических объектах, будут более бдительны и полезны, чем когда они будут не защищены. Охранник, выполняющий часами свои обязанности под проливным дождем или под палящим тропическим солнцем, будут больше беспокоиться о своем состоянии, чем заниматься проверкой пропусков и осмотром машин. Хотелось бы отметить еще один важный момент: вся работа системы корпоративной безопасности снизу доверху строится на доверии. Если СБ не пользуется доверием руководства компании, ее информация ничего не стоит, и вся ее многосторонняя деятельность теряет смысл.

Если сотрудник СБ не пользуется доверием своего непосредственного руководства, то ему здесь не место. Каждый оперативник должен быть абсолютно уверен, что ему полностью доверяют, должен ценить это доверие и никогда им не злоупотреблять. Однако доверие не исключает, а, напротив, подразумевает соответствующий контроль за деятельностью всех элементов системы корпоративной безопасности, а в кадровой политике - разработку таких критериев оценки деятельности каждого отдельного работника, которые бы стимулировали его активность, способствовали объективной оценке его достижений, его служебному росту и не толкали на злоупотребления.

6.5. Корпоративное обучение сотрудников Службы безопасности

Сегодня ведущие сотрудники СБ фирм должны **обладать глубокими знаниями** в следующих областях:

✓ основы менеджмента и маркетинга;

✓ основы банковского дела, бухгалтерский учет;

✓ гражданское и уголовное право;

✓ иностранные языки;

✓ социология, психология;

✓ оперативные техники;

✓ информационно-аналитическая работа;

✓ искусство разведки и контрразведки.

Они также должны:

✓ обладать хорошими организаторскими способностями по созданию СБ и системы комплексных мер, обеспечивающих безопасность фирмы;

✓ уметь коротко и ясно излагать свои мысли, брать интервью;

✓ уметь разрешить конфликтную ситуацию;

✓ осуществлять защиту конфиденциальной информации, втом ; числе и данных в информационно-аналитических системах;

✓ знать и использовать технические средства скрытного наблюдения, проникновения и противодействия;

✓ разбираться в финансовой отчетности фирмы;

✓ налаживать взаимодействие с местными властями и государственными органами в случае расследований происшествий на фирме;

✓ проводить расследования случаев воровства, мошенничества, саботажа и финансовых преступлений на фирме (растраты, хищения, незаконные присвоения денег), осуществлять их профилактику;

✓ готовить документы, содержащие анализ рынка, оценку конкурентов и потенциальных клиентов;

✓ проводить периодическую проверку сотрудников фирмы, имеющих доступ к секретам и т. д.

Программа школы корпоративной учебы службы безопасности предусматривает теоретическую и практическую подготовку сотрудников по следующим **темам**:

✓ организация коммерческой деятельности фирмы;

✓ интеллектуальная собственность фирмы;

✓ недобросовестная конкуренция и промышленный шпионаж;

✓ защита информации на фирме;

✓ информационно-аналитическая работа службы безопасности;

✓ защита собственности фирмы;

✓ основы психической саморегуляции.

Такое обучение в форме лекций, семинаров, практических занятий и тренингов проводится ответственными сотрудниками ведущих отделов фирмы и службы безопасности или приглашенными специалистами.

В плане аудиторных занятий необходимо предусмотреть такие темы:

✓ правовые основы деятельности службы безопасности;

✓ порядок действий личного состава службы безопасности при возникновении экстремальных ситуаций в дневное и ночное время;

✓ характеристики технических средств охранной сигнализации, используемых на данном объекте, и порядок действий в случае их отказа или поломок;

✓ процедура сообщения о правонарушениях представителям закона (обычно в контакт с ними вступает уполномоченный компании, но в экстренных случаях может быть и прямой контакт);

✓ методы выявления факторов внешней и внутренней угрозы безопасности охраняемого объекта;

✓ приемы и уловки, используемые лицами, пытающимися несанкционированно проникнуть на объект;

✓ методы выявления признаков мошенничества и подделки документов;

✓ методы оценки состояния партнера по невербальным сигналам доступа.

6.6. Нештатные структуры Службы безопасности

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства фирмы и службы безопасности могут создаваться отдельные комиссии, выполняющие определенные контрольно-ревизионные функции на временной или постоянной основе, в том числе:

✓ квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);

✓ комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и

телевидении, семинарах, симпозиумах, конференциях и т. п.;

✓ периодические проверочные комиссии для проверки знаний и умения выполнять требования нормативных документов по защите коммерческой тайны, а также для оценки эффективности и надежности защитных мероприятий по обеспечению безопасности фирмы;

✓ специальные группы по аудиту безопасности фирмы.

6.7. Сбор сведений по уголовным делам

Уголовные дела, к расследованию которых подключается служба безопасности, условно можно разделить на **две группы**: возбужденные в связи с совершением преступлений против персонала предприятия и преступления против собственности учредителя.

Причем, если говорить о преступлениях **первой группы**, то обязательным условием сбора сведений о них является их связь с деятельностью предприятия-учредителя. Например, кража личного имущества у сотрудника фирмы сама по себе не обязывает сотрудников службы безопасности подключаться к расследованию этого преступления, однако, в том случае, если среди этого имущества окажутся документы предприятия-учредителя, то ситуация меняется противоположным образом.

Возможно подключение сотрудников службы безопасности к расследованию уголовных дел, по которым работник предприятия является обвиняемым в совершении преступлений, однако, делать это необходимо только по указанию или с разрешения руководителя фирмы.

К наиболее распространенным преступлениям **второй группы** относятся кражи, грабежи, мелкие хищения, поджоги и т.д.

Весьма актуальными для сотрудников службы безопасности стали преступления в сфере экономической деятельности и против интересов службы в коммерческих организациях. Закон допускает сбор сведений по совершенному преступлению только после вынесения постановления о возбуждении уголовного дела. В то же время на практике часто появляется значительный отрезок времени (иногда в несколько суток) между событием преступления, ставшим известным правоохранительным органам и возбуждением уголовного дела. Представляется, что в таких случаях служба безопасности должна, не дожидаясь возбуждения уголовного дела, приступить к сбору сведений по совершенному преступлению, одновременно направить при этом в правоохранительный орган, производящий проверку, письменное уведомление.

Расследование фактов разглашения коммерческой тайны предприятия.

Под **коммерческой тайной** понимается не являющаяся государственным секретом, специально охраняемая собственником (владельцем) управленческая, производственная, научно-техническая, финансовая, торговая и иная деловая

информация. Таким образом, любая конфиденциальная информация, представляющая ценность для предприятия в достижении преимуществ над конкурентами и извлечения прибыли, может стать коммерческой тайной предприятия. Не вдаваясь в методику определения информации, составляющей коммерческую тайну (она описана в многочисленных публикациях) отметим, что таковой она становится только после утверждения руководством предприятия *«Перечня сведений, составляющих коммерческую тайну предприятия»* и объявления его под расписку всем причастным к ней сотрудникам.

Следует, однако, при этом учесть, что в соответствии с Постановлением РСФСР от 05.12.91 г. № 35 *«О перечне сведений, которые не могут составлять коммерческую тайну» (в ред. Постановления Правительста РФ от 03.10.2002 N 731)*, **не могут составлять коммерческую тайну**:

✓ учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

✓ документы, дающие право заниматься предпринимательской деятельностью (документы, подтверждающие факт внесения записей о юридических лицах в Единый государственный реестр юридических лиц, свидетельства о государственной регистрации индивидуальных предпринимателей, лицензии, патенты);

✓ сведения по установленным формам отчетности о финансовохозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

✓ документы о платежеспособности;

✓ сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

✓ документы об уплате налогов и обязательных платежах;

✓ сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

✓ сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

По факту разглашения коммерческой тайны предприятия служба безопасности должна проводить расследование по следующим направлениям:

1) человек;

2) документ;

3) изделие-процесс.

Именно в рамках этой триады (разумеется, при ее конкретизации) расположены каналы утечки информации, поэтому наиболее целесообразно организовать работу

службы безопасности по перечисленным направлениям.

Сбор информации о лицах, заключивших с предприятием контракты.

Предприятие обычно заключает **два типа контрактов**: коммерческий (документ, представляющий собой договор поставки товаров или предоставления услуг) и трудовой (вид трудового договора, заключающегося в письменной форме со своими постоянными или временными работниками).

Одним из договорных условий может быть письменное согласие лица, с кем подписывается контракт, на сбор информации об его биографических и других характеризующих личность данных. При этом в контракте должно быть оговорено, что такого рода сбор информации проводится как до вступления контракта в силу (например, во время прохождения испытательного срока), так и во время его реализации, т.е. до расторжения контракта.

Содержание такой информации о личности проверяемого должно, на наш взгляд, включать следующие сведения:

✓ преступления и административные проступки, совершенные им в прошлом;

✓ судебные процессы по гражданским делам, в которых он выступал в качестве истца или ответчика;

✓ качество исполнения ранее заключаемых договоров с другими партнерами;

✓ аморальные проступки (пьянство, внебрачные связи, наркотики и т.д.);

✓ суждения бывших сослуживцев и руководителей о его профессиональных и моральных качествах;

✓ болезни, которые он перенес ранее;

✓ материальное положение;

✓ случаи увольнения с работы по отрицательным мотивам, не нашедшие отражение в трудовой книжке;

✓ участие в организациях, дискриминирующих по признакам пола, расы, цвета кожи, убеждениям, религиозной и национальной принадлежности;

✓ наличие значительных финансовых накоплений сомнительного происхождения;

✓ необоснованный и нелогичный отказ от продвижения по службе, перевода на новое место работы;

✓ жалобы клиентов и других лиц, контактирующих с проверяемым;

✓ прогулы и частые отвлечения от выполнения служебных обязанностей;

✓ задержки по надуманным предлогам на работе после окончания рабочего дня;

✓ факты отказа от использования очередного отпуска;

✓ результаты различных тестов;

- ✓ семейные проблемы;
- ✓ долги и займы и т.д.

Представляется, что совокупность вышеуказанных сведений в достаточной мере может характеризовать человека и помочь руководству предприятия принять решение о целесообразности дальнейшего с ним сотрудничества.

Поиск утраченного имущества предприятия.

Под **имуществом** предприятия понимается находящиеся в его ведении или собственности материальные ценности, денежные средства в кассе, на расчетном счете и других счетах в банках, нематериальные активы (патенты, лицензии, программы, ноу-хау, брокерские места и т п.).

В узком смысле слова под имуществом предприятия понимаются вещи (материальные ценности). Именно в этом смысле в данном пункте рассматривается утраченное имущество.

Утраченное имущество предприятия условно делится на две категории:

- ✓ ставшее бесхозяйным (т.е. собственник которого неизвестен);
- ✓ утерянное по халатности его сотрудников.

Первую категорию характеризуют следующие **признаки**:

1) имущество утеряно при неизвестных обстоятельствах;

2) информация о пропаже поступает, как правило, с опозданием;

3) закрепление за утерянным имуществом либо не произведено, либо сделано формально;

4) само имущество, за редким исключением, является громоздким или большим (грузовые автомашины, экскаваторы, трубы и т.д.);

5) охрана имущества не выставляется, а при ее наличии передача охраняемого имущества по смене не производится.

Признаки, характеризующие утерянное имущество **по халатности сотрудников**, следующие:

1) его относительно малые габариты или ценные бумаги (калькуляторы, деньги, документы и т.д.);

2) очевидность вины конкретного сотрудника;

3) известны место и время (иногда приблизительно) пропажи;

4) неизвестны способы пропажи имущества.

Объединяет их одно: нанесение материального (иногда значительного) ущерба предприятию. Содержание работы сотрудников службы безопасности в зависимости

от категории утраченного имущества носит различный характер.

Расследование фактов неправомерного использования товарных (фирменных) знаков предприятия.

Товарный знак – это обозначение, способное отличать соответственно товары и услуги одних юридических и физических лиц от однородных товаров и услуг других юридических или физических лиц. Нарушением прав владельца товарного знака признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью товарного знака или товара, обозначенного этим знаком, или обозначения, сходного с ним до степени смешения в отношении однородных товаров. Важнейшей особенностью такого нарушения является его большой территориальный разброс, наличие большого количества потенциальных правонарушителей и сложности с его документированием, что чрезвычайно затрудняет деятельность сотрудников службы безопасности.

Розыск без вести пропавших сотрудников.

Без вести пропавшим считается лицо, исчезнувшее внезапно, без видимых к тому причин, местонахождение и судьба которого остается неизвестной. Все случаи безвестного исчезновения сотрудников можно разделить на **четыре группы**:

✓ связанные с криминальным характером происшедшего (убийство, наезд транспорта со смертельным исходом и т.д.);

✓ обусловленные некриминальным лишением жизни пропавшего (самоубийство, утопление и т.д.);

✓ объективно не зависящие от сознания и воли сотрудников и не носящие криминальный характер (уход из дома вследствие психического заболевания, административный арест и т.д.);

✓ вызванные проблемами личного и служебного характера (семейные неурядицы, ссора с начальством и т.д.).

Сотрудники службы безопасности подключаются к розыску без вести пропавшего сотрудника только в том случае, если есть основания предполагать, что его отсутствие на работе приведет (может привести) к реальному или потенциальному ущербу предприятию. Деятельность службы безопасности по розыску без вести пропавшего сотрудника – это комплекс мероприятий, осуществляемых при тесном взаимодействии с органами внутренних дел с целью установления фактических обстоятельств его исчезновения и фактического местонахождения.

Выявление некредитоспособных партнеров.

Некредитоспособным признается тот партнер, у которого для получения кредита нет предпосылок, подтверждающих способность возвратить его.

Некредитоспособного партнера характеризуют следующие действия:

✓ неаккуратность при расчетах по ранее полученным кредитам;

✓ ухудшение текущего финансового положения;

✓ неспособность при необходимости мобилизовать денежные средства из различных источников;

✓ обналичивание денежных средств в объемах, превышающих размеры фонда зарплаты;

✓ удержание им (без согласия партнера) денежных средств, полученных в качестве кредита или предварительной оплаты,

✓ совершение операций с банковскими документами необеспеченными кредитными ресурсами;

✓ нецелевое использование кредитных средств или их получение по фиктивным документам;

✓ попытка оттянуть выплату денежных средств партнеру при добросовестном выполнении им условий контракта и т.д.

Служба безопасности обязана выявлять некредитоспособных партнеров как до заключения, так и в процессе реализации договора и своевременно информировать об этом руководство предприятия.

Выявление ненадежных деловых партнеров.

Ненадежность делового партнера определяется:

✓ большим количеством сорванных по его вине сделок с другими фирмами;

✓ несвоевременным и некачественным выполнением условий заключенных договоров;

✓ значительным количеством в фирме ранее судимых лиц;

✓ фактами ведения против предприятия-учредителя экономического шпионажа;

✓ использование помощи сотрудников правоохранительных органов, налоговых инспекций и т.д. с целью парализации экономической деятельности своего партнера;

✓ умышленным затягиванием деловых переговоров;

✓ неуважительным отношением к авторскому или патентному праву;

✓ предъявлением к нему значительного количества судебных исков;

✓ наличием большого долга;

✓ непрочной позицией на рынке;

✓ нерегулярной и ненадежной поставкой сырья и товаров;

✓ отсутствием доверия потребителей;

✓ испорченной репутацией среди деловых кругов.

Способность службы безопасности своевременно выявить хотя бы отдельные параметры ненадежности будущих или настоящих деловых партнеров в значительной степени может повлиять на степень экономической безопасности предприятия-учредителя.

Сбор сведений по гражданским делам.

Известно, что в рамках гражданского производства судами рассматриваются:

✓ споры о праве гражданском, затрагивающем права и законные интересы юридического лица (в нашем случае, предприятия);

✓ в предусмотренных законом случаях дел по жалобе на действия административных органов или должностных лиц, совершенные с нарушением их полномочий;

✓ дела об установлении фактов, имеющих юридическое значение, рассматриваемые и разрешаемые судом.

Сбор сведений по гражданским делам служба безопасности осуществляет во взаимодействии с представителем предприятия-учредителя на суде как до, так и во время рассмотрения их на судебных заседаниях.

Необходимость в сборе информации сотрудниками службы безопасности возникает обычно в случаях:

✓ выявления свидетелей и документов;

✓ проверки достоверности информации участников процесса и подлинности доказательств, представленных на суде;

✓ возникновения необходимости проверки наличия основания для отвода в рассмотрении дела;

✓ оказания помощи суду в установлении фактического местонахождения участников процесса;

✓ выявления лиц, оскорбляющих или оклеветавших руководителей предприятия-учредителя;

✓ поиска утаиваемого от суда имущества процессуального противника, необходимого для погашения материального ущерба;

✓ необходимости выявления среди свидетелей лиц, которые в силу своих физических или психических недостатков не способны правильно воспринимать факты или давать о них правильные показания и т.д.

Изучение негативных аспектов рынка.

Под **рынком** понимается сфера товарного обращения, товарооборота, выявляющая и устанавливающая общественно необходимые затраты труда на производство товара. Комплексный анализ рынка проводит специально предназначенная для этого служба предприятия, которая наряду с официальной экономической информацией, использует сведения, представленные службой безопасности.

Такие сведения могут быть сведены в **два блока**:

1) состояние и влияние теневой экономики на рынок;

2) криминальные аспекты рынка.

Теневая экономика (т.е. вся экономическая деятельность, которая по каким-либо причинам не учитывается официальной статистикой и не включается в валовый национальный продукт) состоит из **двух частей**:

1) **экономическая** деятельность, являющаяся вполне легальной, нескрываемой деятельностью, но не подвергающаяся налогообложению и по разным причинам не учитываемая официальной статистикой;

2) **противозаконная**, преднамеренно скрываемая экономическая деятельность.

Изучение **криминальных аспектов** рынка, обычно, включает в себя:

✓ криминологическую зараженность существующих или потенциальных потребителей (клиентов);

✓ криминологическую обстановку на территории функционирования рынка и тенденции его развития;

✓ реакцию сотрудников правоохранительных органов на совершаемые правонарушения, затрагивающие интересы предприятия;

✓ состояние правонарушений в сфере кредитно-финансовой системы;

✓ криминологические последствия введения приватизации;

✓ характеристику правонарушений, совершаемых в отношении товаров и услуг, производимых (предлагаемых) предприятием-учредителем, степень текущего и потенциального материального ущерба предприятию от правонарушений на рынке и т.д.

Оценка риска пребывания и деятельности компании в другой стране.

Многонациональные компании требуют от международной системы если не стабильности, то, по крайней мере, предсказуемости. В бизнесе, который связан с другими странами, нельзя обойтись без риска.

Поэтому ваша цель – справиться с этим риском.

Если ваша компания имеет интересы за границей, необходимо создать группу уменьшения риска, целью которой являлась бы оценка и прогноз политических и экономических изменений в стране, уровня стабильности и насилия и других аспектов.

Это даст вам возможность оценить политический риск в вашей международной деятельности и учесть этот фактор в своих стратегических планах.

Если нет возможности найти специалистов для этого в вашей компании, привлеките экспертов со стороны. Компании, предоставляющие такую помощь, предпринимают попытки вести учет террористических актов, а также оценивают и прогнозируют экономические, социальные и политические условия во всех странах мира.

Важным элементом прогнозирования являются ответы на следующие вопросы:

✓ Как стабильна политическая система страны?

✓ Как долго правительство этой страны будет оставаться у власти?

✓ Существует ли активное политическое насилие в стране? От кого оно исходит? Какие группировки вовлечены? Получают ли они внешнюю помощь? Какие цели они обычно выбирали, и какие операции уже были проведены?

✓ Как близки отношения России с этой страной?

Сбор информации для проведения деловых переговоров.

Основными **стадиями переговоров** являются:

- подготовка к переговорам;
- процесс их ведения;
- анализ результатов переговоров и выполнение достигнутых договоренностей.

Сотрудники службы безопасности участвуют в сборе информации на первой и второй стадиях. При всей условности такого деления служба безопасности должна представлять на различных стадиях руководству предприятия-учредителя свою информацию. Например, в процессе подготовки к переговорам сведения об участниках будущих переговоров, их сильных и слабых сторонах, их позициях и планах ведения переговоров, подготовленных материалах, конкурентоспособности и платежеспособности делового партнера и т.д. Во время проведения переговоров служба безопасности должна поставлять информацию об изменениях позиции партнеров по переговорам, о возможных попытках с их стороны шантажировать, подкупать членов делегации предприятия-учредителя, проведения разведывательных мероприятий в отношении их и т.д.

Защита жизни и здоровья персонала от противоправных посягательств.

Защиту организует служба безопасности либо всего персонала предприятия (во время нахождения его на работе), либо некоторых его категорий (руководители, кассиры и т.д.) в рабочее и, как исключение, в нерабочее время, либо применяются оба варианта. При этом четко определяется время (круглосуточно, только в дневное время и т.д.) проведения охранных мероприятий. Охранники должны быть нацелены, прежде всего на пресечение насильственных преступлений (покушение на убийство, рэкет) и

административных проступков (мелкое хулиганство) в отношении охраняемых лиц. Должны широко применяться технические средства защиты.

Охрана имущества предприятия.

Под **охраной имущества** понимается комплекс оперативно-режимных, организационно-управленческих и инженерно-технических действий, проводимых с целью обеспечения сохранности материально-технических и финансовых средств собственника. Охране подлежат все материальные ценности независимо от их местоположения (внутри или за пределами предприятия).

В то же время существуют объекты первостепенной важности, охране которых необходимо уделять особое внимание, так как именно они чаще всего подвергаются противоправному посягательству.

К таким **объектам** относятся:

- дорогостоящие сырьевые ресурсы (нефть, древесина, золото и т.д.);
- дефицитное оборудование (компьютеры, автозапчасти и т.д.);
- продовольственные и промышленные товары;
- деньги, инвалюта и т.д.;
- наиболее важная и конфиденциальная документация;
- земельные угодья, участки и т.д.

Совершенно очевидно, что охране именно этого имущества должно быть уделено главное внимание.

Обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий.

Обеспечение порядка необходимо:

- во время проведения представительских (выставки, ярмарки и т.д.),
- массовых (спортивные соревнования, концерты и т.д.),
- конфиденциальных (заседание правления, совещания руководителей и специалистов по служебным вопросам и т.д.) мероприятий.

В зависимости от их типа меняется и содержание деятельности службы безопасности. Например, при проведении закрытых совещаний основное внимание уделяется, прежде всего, защите сведений, составляющих коммерческую тайну, на выставках необходимо принимать меры к недопущению кражи или порчи имущества предприятия; при проведении концертов основное внимание уделяется физической безопасности людей и т.д.

Консультирование и представление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности.

В обязанности службы безопасности входит не только консультирование и дача рекомендаций сотрудникам предприятия по вопросам обеспечения безопасности, но и ее реализация. В связи с этим необходимо внести в проект Устава службы безопасности положение об обязанности сотрудников подразделений предприятия выполнять эти рекомендации и определить ответственность (материальную и дисциплинарную) за их невыполнение. Проведение консультаций и рекомендаций по вопросам безопасности, обычно, не выходит за пределы таких ее основных видов, как экономическая, информационная, пожарная, физическая безопасность.

Проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Средства охранно-пожарной сигнализации предназначены для обнаружения попыток проникновения на объект и возникновения пожара, оповещения сотрудников службы безопасности о появлении и нарастании этих угроз и обеспечения контроля доступа на охраняемый объект. Деятельность подразделения службы безопасности, осуществляющего функцию внедрения и эксплуатации охранно-пожарной сигнализации, осуществляется в несколько этапов.

Первый этап (проектирование) предусматривает планирование работ по внедрению и капитальному ремонту средств сигнализации, обследование объекта с целью получения исходных данных для разработки исполнительной проектно-сметной документации; материально-техническое обеспечение монтажных работ.

На **этапе выполнения монтажных работ**, для проведения которых обычно приглашаются специализированные организации, осуществляется технический надзор за качеством их производства, особенно при проведении пусконаладочной работы. Наконец, **последний этап** (эксплуатационное обслуживание) включает в себя:

- ✓ сдачу этих средств в эксплуатацию;
- ✓ планирование эксплуатационных мероприятий и контроль за их исполнением;
- ✓ техническое обслуживание, технический контроль за эксплуатацией средств сигнализации;
- ✓ ремонт приборов и аппаратуры охранно-пожарной сигнализации;
- ✓ материальное обеспечение эксплуатационных нужд;
- ✓ ведение установленной технической документации;
- ✓ сбор и обобщение статистических данных по эксплуатационно-техническому обслуживанию;
- ✓ анализ причин отказов в работе аппаратуры и причин, способствующих совершению краж и пожаров с заблокированных участков объекта.

Краткий обзор основных функций службы безопасности позволяет утверждать, что они органично взаимно дополняют друг друга и в случае их успешной реализации образуют единое «поле» безопасности предприятия-учредителя.

ГЛАВА 7
ПРИМЕНЕНИЕ СИСТЕМ БЕЗОПАСНОСТИ В РАЗЛИЧНЫХ ОТРАСЛЯХ ДЕЯТЕЛЬНОСТИ

7.1. Системы безопасности в торговле

Системы защиты от краж из торговых залов это – комплексное решение, которое включает такие элементы систем безопасности как: цифровая система видеозаписи и видеонаблюдения, система контроля кассовых операций, система контроля антикражных устройств, система контроля доступа.

Применение системы защиты от краж, дает возможность значительно уменьшить потери. Суммарные потери в торговле и сфере услуг составляют около 2% от оборота. Потери могут быть сокращены до 0,2% (на 90%) при использовании специальных охранных систем. Например, система контроля кассовых операций решает задачу предотвращения воровства кассирами в торговле и сфере услуг, отслеживая операции, проводящиеся на кассах и терминалах. Существует система, которая обеспечивает контроль работы противокражных устройств, установленных у входов, выходов, кассовых боксов и терминалов, сокращая процент воровства и потерь в торговле.

Данное оборудование может использоваться в тандеме с системами автоматизации торговли – тем самым обеспечивается интеграция систем безопасности с учетными системами предприятий, повышается их управляемость и экономическая безопасность. Также решения могут интегрироваться с различным оборудованием в супермаркетах (гипермаркетах), например, со счетчиками проходов (people counter), обеспечивая автоматизацию сборки и обработки информации о посетителях торгового предприятия.

Системы защиты от краж из торговых залов служат для надежной защиты товаров от несанкционированного выноса самообслуживания; На товар укрепляют различные защитные элементы (незаметные для вора или которые может снять только сам продавец при помощи специального устройства). На выходе устанавливают сенсорные рамки - антенны, которые подают сигнал (звуковой и световой), при попадании такого элемента в зону их действия. Таким образом, персонал оповещается о попытке кражи. Правильно установленная противокражная система может снизить кражи покупателей, а также помогает администрации в профилактике краж персоналом магазина. При выборе противокражного оборудования необходимо следовать следующим правилам: определить тип товара в свободном доступе, требующий защиты.

Исходя из видов товара необходимо выбрать аксессуары (многоразовые и одноразовые этикетки), оптимальные для его защиты, определить требуемую ширину, защищаемого прохода, подобрать дизайн антенн.

7.2. Проверка и оценка потенциального бизнес-партнера

Рассмотрим более подробно одну из наиболее часто встречающихся в жизни задач – проверка и оценка потенциального партнера или конкурента. Как показывает мировая практика, процедура поиска и изучения (оценки) фирмы-партнера должна быть одной из важнейших составляющих отечественного бизнеса.

Выбирая партнера, важно удостовериться не только в его надежности и добросовестности, но и в оптимальности выбора именно этого партнера, а также проанализировать его на возможность долговременного (перспективного) сотрудничества. Всегда следует учитывать, что внешнее и внутреннее положение предприятия со временем может измениться, поэтому необходимо пополнять и актуализировать информацию о состоянии партнера. В нашей экономической ситуации с предприятием-партнером может произойти все что угодно. Так, в один прекрасный день можно обнаружить, что надежный партнер, с которым компания сотрудничает не один год, перестает выполнять договоры. Компания начинает выяснять, в чем дело. Оказывается: поменялись владельцы (учредители, топ-менеджеры) фирмы. Новые руководители уже по каким-то причинам не заинтересованы в добросовестном выполнении своих обязательств. Или руководство компании-партнера неправильно оценило свою рыночную нишу, выбрало неверную маркетинговую и сбытовую политику, неожиданно прекратились арендные отношения и т.п. Все эти факторы необходимо также учитывать при налаживании деловых контактов с другой фирмой.

Как показывает практика, сложный многоаспектный анализ всех сфер надежности партнера или конкурента довольно непросто осуществить одной службе безопасности даже крупной компании. Поэтому за рубежом достаточно популярны и востребованы услуги специализированных компаний, т.н. «кредит-бюро». Они помогут сделать оценку рыночной ситуации, обзор сектора рынка отдельной отрасли или региона, анализ политической и экономической ситуации. В арсенал их услуг входят: оценка организованной преступности и криминогенной ситуации в отдельных регионах, анализ доступных материалов по отдельным политическим фигурам и руководителям крупных компаний и банков, а также отдельным сферам деловых отношений, таким как вексельное обращение, медицинское страхование и многим другим.

С практической точки зрения, представляют интерес рекомендации по оценке и предотвращению возможных потерь от действий недобросовестных партнеров. Процесс заключения договора может быть разделен на три условных этапа: подготовительный (подготовка к подписанию), основной (процесс определения условий договора), заключительный (оформление и непосредственное подписание). Каждый этап имеет свою специфику в обеспечении экономической безопасности. Но именно на подготовительном этапе задача руководителя - определить свое отношение к предполагаемому договору, или точнее, - к потенциальному партнеру. Особое внимание необходимо уделить следующей информации:

1. Правовая форма, предусмотренная учредительными документами компании-партнера (поскольку все они имеют разную степень ответственности).

2. Подтверждаются ли сведения о государственной регистрации компании

официальными регистрирующими органами (поскольку возможно, что это лицо является фиктивным).

3. Соответствует ли юридический адрес регистрации фактическому. Особое внимание следует обратить на факт наличия у компании-партнера собственного помещения, наличия договора и сроков аренды с арендодателем.

4. Разрешена ли подобная деятельность в уставе компании-партнера, имеется ли лицензия на осуществление данного вида деятельности (так как в противном случае сделка может быть признана недействительной).

5. Организационная форма компании-партнера (количество работающих, структура фирмы, система управления, степень самостоятельности фирмы, наличие филиалов, территориальный охват деятельности).

6. Сведения об управленческом персонале компании (образование, наличие судимости, компетентность, деловая репутация).

7. Рыночной статус (контролируемая доля рынка, имидж фирмы, возможность конкуренции с ней, постоянные контрагенты).

8. Наличие специфической информации (наличие “теневого оборота”, участие в нелегальных сделках, связи с преступными группировками и т.п.).

Полномочия самого подписанта (лишь первый руководитель на основании устава вправе заключать договор без доверенности). Заключающее сделку предприятие может оказаться уже ликвидированным, а подписант - подставным лицом или откровенным мошенником. Не стесняйтесь спросить паспорт и переписать из него все данные. Не доверяйте визиткам и удостоверениям.

Если контракт «серьезный», то следует внимательно проанализировать учредительные и иные документы контрагента, желательно также произвести их предварительную экспертизу. Криминалистическая экспертиза документов производится прежде всего на предмет установления их подлинности и отсутствия признаков подделки, таких как: подчистки, дописки, травление, допечатки на пишущих машинках, подделки печатей и штампов, подделки подписей.

В особых случаях запрашивайте у потенциального партнера отдельные финансовые документы. Например, для контролирующих и правоохранительных органов индикаторами низкого уровня экономической безопасности и наличия теневой деятельности на предприятии служат отчетные экономические показатели. В большинстве случаев манипуляция ими затруднена или невозможна в принципе. К таким показателям относятся: низкая заработная плата, реализация продукции через посредников по заниженным ценам, низкие налоговые поступления, низкий оборот, регулярные крупные сделки с мелкими фирмами, высокий уровень потребления электроэнергии и т.п.

При заключении любого возмездного договора (когда придется отдавать деньги по предоплате) убедитесь в наличии и качестве товара и т.п., проверьте подлинники документов контракта.

После сбора общей информации о компании-партнере необходимо проанализировать полученные сведения и определить степень ее надежности как

потенциального контрагента. Для этого используются методы рейтинговой оценки либо принимается решение на основании положительной информации по всем (или большинству) аспектам ее деятельности.

В самом общем виде все потенциальные партнеры по степени надежности могут быть разделены на три группы. Первая группа – наиболее надежные партнеры. Вся собранная информация по вышеназванным критериям является положительной - это позволяет сделать вывод о том, что данный партнер выполняет свои обязательства и имеет высокую исполнительскую дисциплину по совершаемым сделкам.

Вторая группа – партнеры средней степени надежности. Информация свидетельствует, что в большинстве случаев партнер старается выполнять свои обязательства, хотя имели место единичные нарушения условий сделок.

Третья группа – контрагенты с низкой степенью надежности. Они, как правило, не выполняют взятых на себя обязательств, используют нелегальные методы в своей деятельности, зачастую занимаются запрещенными видами деятельности, либо связаны с организованными преступными группировками.

Рекомендовать универсальные методы, надежно защищающие от мошенничества партнеров, невозможно из-за многообразия жульнических приемов. Наиболее важными являются следующие методы защиты от мошенников.

Не спешите расставаться с собственными деньгами. Стремитесь оплачивать товар только после его поставки вам. В крайнем случае выставляйте аккредитив с выгодными для вас условиями его раскрытия (после поставки товара). Вместе с тем существует вероятность подделки документов, необходимых для раскрытия аккредитива.

Если вы провели с новым партнером одну-две небольшие сделки, не считайте, что обязательно будет удачной и третья, крупная сделка. Особенно в случае, если при совершении крупной сделки вашими деньгами будет распоряжаться партнер.

При заключении договора о совместной деятельности предусмотрите ваше обязательное участие во всех основных операциях по совместной деятельности, ваш жесткий контроль за расходованием средств и распределением доходов.

В договоре четко оговаривайте свои экономические интересы. Если контракт не будет выполнен, по условиям договора стремитесь получить максимальную компенсацию.

Поступайте осторожно, если вам будут предлагать чрезвычайно выгодные условия договора.

При заключении договоров на покупку товара и его продажу контролируйте оговариваемые размеры получаемых и выплачиваемых штрафных санкций в случае срыва договоров.

Если партнер ссылается на солидных учредителей, проверьте это в учредительном договоре.

Проверьте паспорт и полномочия лица, подписывающего с вами договор, а также совпадение названия предприятия-партнера в тексте договора, в других документах и на печати.

В тексте договора должны отсутствовать ссылки на обязательства других юридических и физических лиц, кроме подписавших договор.

Необходимо быть особенно внимательным в случае, если договор заключается от имени известной фирмы, а деньги направляются в адрес другого предприятия (даже если последнее называет себя дочерней структурой или региональным представителем известной фирмы).

Проверяйте предоставляемые залоги на предмет их возможного многократного перезакладывания.

При предоставлении вам поручительств (гарантий) других предприятий или организаций проверьте состоятельность поручителя (гаранта) и выясните, давал ли он вообще предоставленную вам гарантию.

В счетах-фактурах, в актах приемки-сдачи работ и в накладных всегда проверяйте соответствие указанного в документах и фактического количества и качества поставляемых товаров, а также объемов выполненных работ и услуг.

Контролируйте своих работников, не создавайте им условий, когда они могут “перепродаться” другой фирме.

7.3. Система защиты коммерческого предприятия

Количественный и качественный анализ угроз позволяет сделать вывод о том, что надежная защита экономики любой компании возможна только при комплексном и системном подходе к ее организации.

К числу основных задач СЭБ любой коммерческой структуры относятся:

- защита законных прав и интересов предприятия и его сотрудников;
- сбор, анализ, оценка данных и прогнозирование развития обстановки;
- изучение партнеров, клиентов, конкурентов, кандидатов на работу в компании;
- своевременное выявление возможных устремлений к предприятию и его сотрудникам со стороны источников внешних угроз безопасности;
- недопущение проникновения на предприятие структур экономической разведки конкурентов, организованной преступности и отдельных лиц с противоправными намерениями;
- противодействие техническому проникновению в преступных целях;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников предприятия в ущерб его безопасности;
- защита сотрудников предприятия от насильственных посягательств;

- обеспечение сохранности материальных ценностей и сведений, составляющих коммерческую тайну предприятия;
- добывание необходимой информации для выработки наиболее оптимальных управленческих решений по вопросам стратегии и тактики экономической деятельности компании;
- физическая и техническая охрана зданий, сооружений, территории и транспортных средств;
- формирование среди населения и деловых партнеров благоприятного мнения о предприятии, способствующего реализации планов экономической деятельности и уставных целей;
- возмещение материального и морального ущерба, нанесенного в результате неправомерных действий организаций и отдельных лиц;
- контроль за эффективностью функционирования системы безопасности, совершенствование ее элементов.

С учетом перечисленных задач, условий конкурентной борьбы, специфики бизнеса предприятия строится его система экономической безопасности. Необходимо отметить, что СЭБ каждой компании также сугубо индивидуальна. Ее полнота и действенность во многом зависят от имеющейся в государстве законодательной базы, выделяемых руководителем предприятия материально-технических и финансовых ресурсов, понимания каждым из сотрудников важности обеспечения безопасности бизнеса, а также от знаний и практического опыта начальника СЭБ, непосредственно занимающегося построением и поддержанием в «рабочем состоянии» самой системы.

Построение СЭБ предприятия должно осуществляться на основе соблюдения принципов:

- законности;
- прав и свобод граждан;
- централизованного управления;
- компетентности;
- конфиденциальности;
- разумной достаточности, соответствия внешним и внутренним угрозам безопасности;
- комплексного использования сил и средств;
- самостоятельности и ответственности за обеспечение безопасности;
- передовой материально-технической оснащенности;
- корпоративной этики;
- координации и взаимодействия с органами власти и управления.

К основным элементам СЭБ предприятия относятся:

1) защита коммерческой тайны и конфиденциальной информации;

2) компьютерная безопасность;

3) внутренняя безопасность;

4) безопасность зданий и сооружений;

5) физическая безопасность;

6) техническая безопасность;

7) безопасность связи;

8) безопасность хозяйственно-договорной деятельности;

9) безопасность перевозок грузов и лиц;

10) безопасность рекламных, культурных, массовых мероприятий, деловых встреч и переговоров;

11) противопожарная безопасность;

12) экологическая безопасность;

13) радиационно-химическая безопасность;

14) конкурентная разведка;

15) информационно-аналитическая работа;

16)пропагандистское обеспечение, социально-психологическая, предупредительно-профилактическая работа среди персонала и его обучение по вопросам экономической безопасности;

17) экспертная проверка механизма системы безопасности.

В наши дни все большую актуальность приобретает защита интересов предприятия от противоправной деятельности коррумпированных представителей контролирующих и правоохранительных органов. В связи с этим, данное направление работы многими начальниками служб экономической безопасности коммерческих структур выделяется в качестве отдельного элемента СЭБ.

Основной смысл подобной системы состоит в том, что она должна носить упреждающий характер, а основными критериями оценки ее надежности и эффективности являются:

- обеспечение стабильной работы предприятия, сохранности и приумножения финансов и материальных ценностей;

- предупреждение кризисных ситуаций, в том числе различных чрезвычайных происшествий, связанных с деятельностью «внешних» и/или «внутренних» недоброжелателей.

Особенностью и, одновременно, сложностью при построении системы экономической

безопасности является тот факт, что ее действенность практически полностью зависит от человеческого фактора. Как показывает практика, даже при наличии на предприятии профессионально подготовленного начальника службы безопасности, современных технические средств, Вы не добьетесь желаемых результатов до тех пор, пока в Вашем коллективе каждый сотрудник не осознает важность и необходимость внедряемых мер экономической безопасности.

А они будут не популярны:

- кто-то утратит возможность в рабочее время или после работы развлекаться в Интернете, скачивать музыку и иную информацию, читать книги в электронном варианте и т.д.;

- кому-то покажется в тягость один раз в неделю менять пароль на своем компьютере;

- кто-то посчитает ниже своего достоинства всякий раз подниматься для того, чтобы уничтожить черновик в бумагорезательной машинке, убрать со стола документы и закрыть окно после окончания рабочего дня, опечатывать и сдавать свой рабочий кабинет под роспись в журнале службе охраны;

- у кого-то исчезнет возможность приводить на работу (в том числе и по выходным дням) своих друзей либо бахвалиться на стороне личными достижениями в работе или успехами фирмы;

- некоторые не смогут использовать служебные автотранспорт и мобильный телефон в личных целях, а также часами вести личные разговоры по служебным проводным каналам телефонной связи и т.д.

Поэтому для юридически правильного, эффективного и всестороннего использования СЭБ в защите интересов предприятия от всех видов недоброжелателей требования по обеспечению безопасности бизнеса излагаются в соответствующих приказах руководителя, трудовых договорах с сотрудниками и их должностных обязанностях, специальных инструкциях, положениях, контрактах с деловыми партнерами и т.д. После чего доводятся до персонала под роспись в процессе занятий и инструктажей.

В вопросах экономической безопасности как никогда важна роль и понимание актуальности проблемы в первую очередь самим руководителем предприятия. Директор и, при наличии, начальник службы безопасности, должны пропагандировать среди персонала одно из основных корпоративных правил: «Фирма - это твоя вторая семья. Предприятие дает всем сотрудникам работу, материальные блага, перспективы служебного роста и т.д. В связи с этим задача каждого сотрудника — приумножать успех и материальное положение компании (как и своей семьи). Ведь успех предприятия - это стабильность и перспективы его персонала».

Вместе с тем, как показывает практика, кто-то из Ваших сотрудников может не выполнять установленные в компании требования или допускать ошибки по забывчивости, кто-то по неаккуратности, а кто-то - из мести. У кого-то могут возникнуть финансовые затруднения в связи с болезнью близких или в связи с проигрышем в казино, и он решит их «компенсировать» за счет фирмы. Кто-то посчитает, что был незаслуженно наказан директором, что давно достоин повышения в должности или что его вклад в деятельность компании заслуживает гораздо более высокой зарплаты, а руководство этого не замечает и т.д.

Словом, с возрастом, изменением социального статуса, материального благосостояния, появлением вредных наклонностей, а также при возникновении некоторых объективных обстоятельств люди могут меняться либо вести себя неадекватно.

При этом необходимо понимать, что в вопросах обеспечения экономической безопасности «второстепенных» должностных лиц нет, а есть только особенности (в связи с выполняемыми каждым из сотрудников функциями и обязанностями).

Секретарь - наверное никто не будет возражать, что эта категория обладает серьезным объемом самой разноплановой информации о фирме.

Уборщица может похитить с рабочего стола директора документ с важной информацией или переписать, запомнить, ксерокопировать его содержание, добросовестно выбросить из мусорной корзины неуничтоженные документы либо документы, уничтоженные таким образом, что не составляет никакого труда их восстановить.

Охранник в состоянии сделать все то же самое, а в ночное время и выходные дни у него появляется дополнительная возможность впустить в офис посторонних, которые, в свою очередь, могут Вам навредить (начиная от банального хищения документов и имущества и заканчивая постановкой в Вашем кабинете подслушивающей техники или «перекачки» закрытой информации из вашего компьютера).

С учетом изложенного, можно сделать вывод о том, что СЭБ предприятия только тогда будет соответствовать предъявляемым к ней требованиям, когда весь персонал понимает важность обеспечения безопасности компании и сознательно выполняет все установленные указанной системой требования. Достигается же данная цель в результате проведения непрерывной, кропотливой воспитательной и профилактической работы с сотрудниками предприятия, их обучения и специальной подготовки по вопросам действующего законодательства и различным аспектам экономической безопасности.

Алгоритм построения

После получения информации о том, что такое система экономической безопасности предприятия и ее структурные элементы, принципы построения и задачи, резонно возникает вопрос: «Каким образом СЭБ строится?»

У каждого начальника службы безопасности свой подход к решению данной проблемы.

С нашей точки зрения, алгоритм построения СЭБ должен включать в себя следующие этапы:

1) Изучение специфики бизнеса предприятия, занимаемого им сегмента на рынке, штатного расписания, знакомство с персоналом компании.

2) Анализ внешних и внутренних угроз экономике предприятия. Получение информации о возможно имевших место ранее кризисных ситуациях, их причинах и результатах разрешения.

3) Проведение аудита имеющихся (ранее введенных) мер по обеспечению

безопасности и анализ их соответствия выявленным угрозам.

4) Моделирование новой системы экономической безопасности предприятия:

- план устранения выявленных в процессе аудита замечаний;

- предложения по совершенствованию СЭБ, расчет всех видов необходимых дополнительных ресурсов;

- планируемые ежемесячные затраты (бюджет) на обеспечение функционирования СЭБ.

5) Утверждение руководителем предприятия модели новой СЭБ и бюджета на ее поддержание.

6) Непосредственное построение СЭБ предприятия.

7) Экспертная оценка действенности построенной СЭБ, доводка ее до совершенства.

Вместе с тем, даже если сегодня на Вашем предприятии отработана действенная СЭБ, все равно не стоит обольщаться и «почивать на лаврах».

Система экономической безопасности — это живой организм, который требует постоянного контроля, совершенствования и управления им в связи с:

- изменениями в действующем законодательстве государства;

- развитием компании и избранием ею новых направлений хозяйственной деятельности;

- увеличением количества персонала, изменениями в штатном расписании фирмы;

- изменением перечня сведений, составляющих коммерческую тайну и конфиденциальную информацию предприятия;

- необходимостью совершенствования телефонной и компьютерной сетей компании;

- изобретением недоброжелателями новых технологий промышленного шпионажа и мошенничества;

- появлением на рынке недобросовестных конкурентов и изменением форм и методов их противоправной деятельности;

- состоянием криминогенной обстановки в регионе и т.д.

7.4. Обеспечения комплексной безопасности на предприятиях электроэнергетики

Прежде всего, следует выделить основные принципы построения систем безопасности:

- принцип законности.

Реализация этого принципа осуществляется за счёт тщательного соблюдения и выполнения при разработке и построении систем безопасности требований

действующего законодательства;

- принцип своевременности.

Реализуется принятием упреждающих мер обеспечения безопасности;

- принцип совмещения комплексности и эффективности и экономической целесообразности.

Реализуется за счёт построения системы безопасности, обеспечивающей надежную защиту комплекса имеющихся на предприятии ресурсов от комплекса возможных угроз с минимально возможными, но не превышающими 20% стоимость защищаемых ресурсов затратами.

- принцип модульности.

Реализуется за счёт построения системы на базе гибких аппаратно-программных модулей. Модульность программы позволяет ей работать в двух режимах – дежурном и инсталляции, позволяет наращивать, изменять конфигурацию системы и вносить другие изменения без замены основного оборудования;

- принцип иерархичности.

Реализуется за счёт построения многоуровневой структуры, состоящей из оборудования Центра, оборудования среднего звена и объектового оборудования. Модульность и иерархичность позволяют разрабатывать системы безопасности для самого высокого организационно - структурного уровня;

- принцип преимущественно программной настройки.

- Реализуется за счёт использования для перенастройки оборудования способ ввода новых управляющих программ – модулей;

- принцип совместимости технологических, программных, информационных, конструктивных, энергетических и эксплуатационных элементов в применяемых технических средствах.

Технологическая совместимость обеспечивает технологическое единство и взаимозаменяемость компонентов. Это требование достигается унификацией технологии производства составных элементов системы. Информационная совместимость подсистем систем безопасности обеспечивает их оптимальное взаимодействие при выполнении заданных функций. Для её достижения используются стандартные блоки связи, выдерживается строгая регламентация входных и выходных параметров модулей на всех иерархических уровнях системы, входных и выходных сигналов для управляющих воздействий.

Комплексные системы безопасности – это совокупность взаимоувязанных организационных мероприятий (мер, способов) и технических средств, объединённых каналами связи; и совокупность мероприятий обеспечивающих поддержание безопасного состояния объекта, обнаружение и ликвидацию максимально полного перечня (комплекса) угроз жизни, здоровью, среде обитания, имуществу и информации; совокупность имеющая общие средства сбора и обработки информации и управления.

В состав, в качестве технических средств обеспечения безопасности, входит комплексная система технических средств охраны - совокупность технических средств и/или систем (тревожной, охранной и охранно-пожарной сигнализации, контроля и управления доступом, видеонаблюдения и др.), обеспечивающих выполнение комплекса задач системы безопасности.

В типовой состав оснащения объектов энергетики входят следующие технические средства и системы:

- сбора, обработки и отображения информации (ССОИ);
- охранной и тревожной сигнализации (ОС и ТС);
- управления и контроля доступом (СКУД);
- телевизионного видеонаблюдения и видеорегистрации (ТСВ);
- охранно-пожарной сигнализации (ОПС);
- оповещения о пожаре и дымоудаления (ОС и ДУ);
- пожаротушения (ПТ);
- защиты от несанкционированного съёма информации (ЗНСИ);
- бесперебойного электропитания (СБП);
- оперативной связи, оповещения и радиотрансляции;
- средств технической укреплённости (СТУ).

Количество и состав подсистем может варьироваться в зависимости от потребностей объекта.

Типовые задачи:

- защита жизни и здоровья лиц, находящихся на объекте;
- защита материальных и информационных ценностей;
- защита собственных ресурсов и технических средств при попытках несанкционированного доступа к ним;
- организация доступа сотрудников и посетителей на территорию объекта и в режимные помещения;
- табельный учет;
- обнаружение и регистрация фактов несанкционированного проникновения нарушителя на территорию объекта, в здания и режимные помещения, а также оповещение охраны или службы безопасности о нештатных ситуациях;
- организация тревожно-вызывной сигнализации и тревожного оперативного оповещения;

- наблюдение за территорией, прилегающей к зданиям объекта, и за транспортными потоками на ней с созданием видеоархива;
- Защищённость объектов энергетики, особенно от проникновения посторонних лиц, должна быть высокой.

Отдельное внимание следует уделить безопасности гидротехнических сооружений, поскольку любые производственные циклы этой отрасли являются опасными и могут создавать угрозу для экологии, здоровья и жизни людей. Кроме этого, обеспечение безопасности и надёжности гидроэлектростанций (ГЭС) является требованием законодательной базы Российской Федерации.

В настоящее время комплексная защита ГЭС строится преимущественно на основе датчиковых средств охраны, основанных на различных физических принципах, которые не всегда и не во всех условиях гарантируют надежную работу в условиях ГЭС.

Так, например, изменение уровня воды зачастую приводит к нестабильной работе датчиковых систем, которые настраиваются на определённый уровень воды, и потенциальный нарушитель может проникнуть на объект, воспользовавшись приливом или отливом.

В настоящее время на рынке систем безопасности появилась Радиолокационная система (РЛС) охраны периметра и территории объектов, которая соответствует высоким требованиям и позволит повысить безопасность ГЭС. РЛС предназначены для круглосуточной, всепогодной охраны объектов посредством радиолокационного наблюдения периметра и территории, обнаружения движущихся целей, измерения их координат и скорости, распознавания класса и автосопровождения обнаруженных целей. РЛС может интегрироваться с поворотной видеокамерой (тепловизором) и выполнять функции целеуказания, при этом получаемое оператором видео (тепловизионное) изображение достаточно для верификации нарушителя (или ситуации) и принятия правильного решения. Особенностью применения РЛС является работа в местах постоянного присутствия людей, поэтому уровень электромагнитного излучения должен быть предельно низок и соответствовать требованиям СанПиН.

РЛС позволяет обеспечить охрану водосброса, шлюза и прилегающей территории ГЭС. Система в автоматическом режиме информирует оператора о проникновении нарушителя на объект как со стороны суши, так и со стороны прилегающей акватории.

На основе РЛС можно создавать сети радиолокационных станций для охраны территорий и периметра большой протяжённости. В состав системы могут также включаться неподвижные и поворотные видеокамеры и тепловизоры, любые датчиковые системы. Информация о целевой обстановке отображается на автоматизированном рабочем месте оператора со всех РЛС, видеокамер и тепловизоров, что позволяет контролировать весь периметр и территорию объекта из единого центра.

Общий уровень безопасности объектов зависит не только от использования высокотехнологичных систем, но и от способности этих систем обмениваться информацией в единой базе данных, обеспечивая принципиально более высокий уровень защиты.

Новым направлением в обеспечении безопасности объектов энергетики является взаимодействие с разработчиками эксклюзивных охранных систем с целью обеспечения комплексными системами безопасности.

Телевизионное видеонаблюдение и видеорегистрация (ТСВ)

На данный момент многие предприятия, устанавливая системы ТСВ, не учитывают расширяющихся потребностей и увеличения мощностей. Лучшим предлагается использование видеосерверов. Так как система видеосерверов позволяет организовывать и расширять системы до бесконечности.

Система строится на видеосерверах Пандора российского производства, которые позволяют не только работать с массивами видео, но и транслировать реальное видео в компьютерную сеть предприятия. Разграничивать права доступа и просмотра. А также, при необходимости, передавать сигнал на удалённые терминалы по сетям Интернет. Качество видео определяется , в этом случае, только техническими характеристиками сетей.

Охранная и тревожной сигнализации (ОС и ТС)

Оповещение о пожаре и дымоудаление (ОП и ДУ), пожаротушение (ПТ)

Охранная и тревожная сигнализации, оповещение о пожаре и дымоудаление строятся на оборудовании российского производства компании Болид, что существенно снижает стоимость ОС,ТС, ОП и ДУ. Упрощает работу при монтаже, дальнейшем обслуживании и сервисной поддержке.

Управление и контроль доступом (СКУД)

Управление и контроль доступом, в основном, организованы на платформе Форсек. СКУД – это не только система, которая позволяет контролировать проход в здание или проезд на территорию предприятия, но и система позволяющая организовать доступ к отдельным помещениям, этажам и коридорам. СКУД это не только разграничение доступа, но и система, позволяющая систематизировать и учитывать рабочее время сотрудников предприятия, въезд и выезд автотранспорта. При использовании программного обеспечения Senesys-Avto мы обеспечиваем не только распознавания автомобильного номера, но и распознавание автотранспорта по внешнему виду, для исключения случаев смены номеров на автотранспорте.

Новым направлением в обеспечении безопасности предприятий является объединение всех систем в единый Ситуационный центр, который мог бы проводить мониторинг всех систем одновременно и принимать решения по возникшим ситуациям.

7.5. Система информационной безопасности предприятия

Главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов Заказчика от противоправных посягательств,

недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта. Другой целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Достижение заданных целей возможно в ходе решения следующих основных задач:

- отнесение информации к категории ограниченного доступа (служебной тайне);
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития;
- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения информационной безопасности на достижение стратегических целей.

Модель построения системы информационной безопасности

При выполнении работ можно использовать следующую модель построения системы информационной безопасности (рисунок 4), основанную на адаптации ОК (ISO 15408) и проведении анализа риска (ISO 17799).

Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 "Информационная технология - методы защиты - критерии оценки информационной безопасности", стандарту ISO/IEC 17799 "Управление информационной безопасностью", и учитывает тенденции развития отечественной нормативной базы (в частности, Гостехкомиссии РФ) по вопросам информационной безопасности.

Представленная модель информационной безопасности - это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рисунок 4. Модель построения системы информационной безопасности предприятия

Рассматриваются следующие объективные факторы:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- риск - фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

Методика проведения аналитических работ

Предлагаемая методика позволяет:

- полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасностью;

- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем;
- обеспечить проведение работ в сжатые сроки;
- представить обоснование для выбора мер противодействия;
- оценить эффективность контрмер, сравнить различные варианты контрмер.

Определение границ исследования

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные. Примерами внешних элементов являются сети связи, внешние сервисы и т. п.

Построение модели информационной технологии

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствие с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т. д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

Выбор контрмер

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут являться рекомендации по проведению регулярных проверок эффективности системы защиты.

Управление рисками

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Оценка достигаемой защищенности

В завершение работ, можно будет определить меру гарантии безопасности информационной среды Заказчика, основанную на оценке, с которой можно доверять информационной среде объекта.

Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на:

- вовлечении в процесс оценки большего числа элементов информационной среды объекта Заказчика;
- глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения;
- строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Методология анализа рисков

Цель процесса оценивания рисков состоит в определении характеристик рисков в информационной системе и ее ресурсах. На основе таких данных выбираются необходимые средства управления ИБ.

Процесс оценивания рисков содержит несколько этапов:

- описание объекта и мер защиты;
- идентификация ресурса и оценивание его количественных показателей (определение потенциального негативного воздействия на бизнес);
- анализ угроз информационной безопасности;
- оценивание уязвимостей;
- оценивание существующих и предполагаемых средств обеспечения информационной безопасности;
- оценивание рисков.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация, и зависит от:

- показателей ценности ресурсов;
- вероятностей нанесения ущерба ресурсам (выражаемых через вероятности реализации угроз для ресурсов);
- степени легкости, с которой уязвимости могут быть использованы при возникновении угроз (уязвимости системы защиты);
- существующих или планируемых средств обеспечения ИБ.

Расчет этих показателей выполняется на основе математических методов, имеющих

такие характеристики, как обоснование и параметры точности метода.

Построение профиля защиты

На этом этапе разрабатывается план проектирования системы защиты информационной среды Заказчика. Производится оценка доступных средств, осуществляется анализ и планирование разработки и интеграции средств защиты (рисунок 5).

Рисунок 5. Возможный алгоритм оценивания информационных рисков

Необходимым элементом работы является утверждение у Заказчика допустимого риска объекта защиты.

Обеспечение повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике без-опасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

Работа по построению плана защиты объекта начинается с построения профиля защиты данного объекта. При этом часть этой работы уже была проделана при проведении анализа рисков.

Формирование организационной политики безопасности

Прежде чем предлагать какие-либо технические решения по системе информационной безопасности объекта, предстоит разработать для него политику безопасности.

Собственно организационная политика безопасности описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) объекта окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Шагами построения организационной политики безопасности являются:

- внесение в описание объекта автоматизации структуры ценности и проведение анализа риска;
- определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Организационная политика безопасности оформляется в виде отдельного документа, который согласовывается и утверждается Заказчиком.

Условия безопасного использования ИТ

Предполагается, что система обеспечения безопасности объекта Заказчика, соответствующая выбранному профилю защиты, обеспечит требуемый уровень безопасности только в том случае, если она установлена, управляется и используется в соответствие с выработанными правилами. Операционная среда должна управляться согласно принятой для данного профиля защиты нормативной документации, а также инструкциям администраторов и пользователей.

Выделяются следующие виды условий безопасного использования ИТ:

- физические условия;
- условия для персонала;
- условия соединений.

Физические условия касаются размещения ресурсов объекта, а также защиты аппаратных средств и программного обеспечения, критичных к нарушению политики безопасности.

Условия для персонала содержат организационные вопросы управления безопасностью и отслеживания полномочий пользователей.

Условия соединений не содержат явных требований для сетей и распределенных систем, но, например, условие равенства положения означает наличие единой

области управления всей сетью объекта.

Условия безопасного использования объекта автоматизации оформляются в виде отдельного документа, который согласовывается и утверждается Заказчиком.

Формулирование целей безопасности объекта

В этом разделе профиля защиты дается детализованное описание общей цели построения системы безопасности объекта Заказчика, выражаемое через совокупность факторов или критериев, уточняющих цель. Совокупность факторов служит базисом для определения требований к системе (выбор альтернатив).

Факторы безопасности, в свою очередь, могут распределяться на технологические, технические и организационные.

Определение функциональных требований безопасности

Функциональные требования профиля защиты определяются на основе набора хорошо известных, отработанных и согласованных функциональных требований безопасности. Все требования к функциям безопасности можно разделить на два типа: управление доступом к информации и управление потоками информации.

На этом этапе предстоит правильно определить для объекта компоненты функций безопасности. Компонент функции безопасности описывает определенный набор требований безопасности - наименьший выбираемый набор требований безопасности для включения в профиль защиты. Между компонентами могут существовать зависимости.

Требования гарантии достигаемой защищенности

Структура требований гарантии аналогична структуре функциональных требований и включает классы, семейства, компоненты и элементы гарантии, а также уровни гарантии. Классы и семейства гарантии отражают такие вопросы, как разработка, управление конфигурацией, рабочая документация, поддержание этапов жизненного цикла, тестирование, оценка уязвимости и другие вопросы.

Требования гарантии достигаемой защиты выражаются через оценки функций безопасности СИБ объекта. Оценка силы функции без-опасности выполняется на уровне отдельного механизма защиты, а ее результаты позволяют определить относительную способность соответствующей функции безопасности противостоять идентифицированным угрозам. Исходя из известного потенциала нападения, сила функции защиты определяется, например, категориями "базовая", "средняя", "высокая".

Потенциал нападения определяется путем экспертизы возможностей, ресурсов и мотивов побуждения нападающего.

Уровни гарантии. Предлагается использовать табличную сводку уровней гарантированности защиты. Уровни гарантии имеют иерархическую структуру, где каждый следующий уровень предоставляет большие гарантии и включает все требования предыдущего.

Формирование перечня требований

Перечень требований к системе информационной безопасности, эскизный проект, план защиты (далее - техническая документация, ТД) содержит набор требований безопасности информационной среды объекта Заказчика, которые могут ссылаться на соответствующий профиль защиты, а также содержать требования, сформулированные в явном виде.

В общем виде разработка ТД включает:

- уточнение функций защиты;
- выбор архитектурных принципов построения СИБ;
- разработку логической структуры СИБ (четкое описание интерфейсов);
- уточнение требований функций обеспечения гарантоспособности СИБ;
- разработку методики и программы испытаний на соответствие сформулированным требованиям.

Оценка достигаемой защищенности

На этом этапе производится оценка меры гарантии безопасности информационной среды объекта автоматизации. Мера гарантии основывается на оценке, с которой после выполнения рекомендованных мероприятий можно доверять информационной среде объекта.

Базовые положения данной методики предполагают, что степень гарантии следует из эффективности усилий при проведении оценки безопасности.

Увеличение усилий оценки предполагает:

- значительное число элементов информационной среды объекта, участвующих в процессе оценивания;
- расширение типов проектов и описаний деталей выполнения при проектировании системы обеспечения безопасности;
- строгость, заключающуюся в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

В целом рассмотренная выше методика позволяет оценить или переоценить уровень текущего состояния информационной безопасности предприятия, выработать рекомендации по обеспечению (повышению) информационной безопасности предприятия, снизить потенциальные потери предприятия или организации путем повышения устойчивости функционирования корпоративной сети, разработать концепцию и политику безопасности предприятия, а также предложить планы защиты конфиденциальной информации предприятия, передаваемой по открытым каналам связи, защиты информации предприятия от умышленного искажения (разрушения), несанкционированного доступа к ней, ее копирования или использования.

7.6. Разработка и реализация политики безопасности предприятия

Подготовительный этап

Обеспечение комплексной безопасности является необходимым условием функционирования любой компании. Эта "комплексность" заключается, прежде всего, в продуманности, сбалансированности защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Всякой успешной деятельности должен предшествовать этап планирования. Шахматисты знают, что, не создав четкого плана, выиграть партию у сколько-нибудь серьезного соперника невозможно. А соперник — "промышленный шпион" — у нас достаточно серьезный. Планирование обеспечения безопасности заключается в разработке политики безопасности.

Вначале необходимо провести аудит информационных процессов фирмы, выявить критически важную информацию, которую необходимо защищать. Иногда к этому делу подходят однобоко, полагая, что защита заключается в обеспечении конфиденциальности информации. При этом упускаются из виду необходимость обеспечения защиты информации от подделки, модификации, парирования угроз нарушения работоспособности системы. Например, обиженный чем-то программист может вставить деструктивную закладку в программное обеспечение, ко-торая сотрет ценную базу данных уже намного позднее времени его увольнения. Аудит информационных процессов должен заканчиваться определением перечня конфиденциальной информации предприятия, участков, где эта информация обращается, допущенных к ней лиц, а также последствий утраты (искажения) этой информации.

После этого становится ясно, что защищать, где защищать и от кого защищать: ведь в подавляющем случае инцидентов в качестве нарушителей будут выступать — вольно или невольно — сами сотрудники фирмы. На самом деле, с этим ничего нельзя поделать: это надо принять как данность. Различным угрозам безопасности можно присвоить вероятности их реализации. Умножив вероятность реализации угрозы на причиняемый этой реализацией ущерб, получим риск угрозы. После этого можно приступать к разработке политики безопасности.

Содержание политики безопасности

Политика безопасности — это документ "верхнего" уровня, в котором должно быть указано:

- ответственные лица за безопасность функционирования фирмы;
- полномочия и ответственность отделов и служб в отношении безопасности;
- организация допуска новых сотрудников и их увольнения;
- правила разграничения доступа сотрудников к информационным ресурсам;

- организация пропускного режима, регистрации сотрудников и посетителей;
- использование программно-технических средств защиты;
- другие требования общего характера.

Таким образом, политика безопасности — это организационно-правовой и технический документ одновременно. При ее составлении надо всегда опираться на принцип разумной достаточности и не терять здравого смысла.

Например, в политике может быть указано, что все прибывающие на территорию фирмы сдают мобильные телефоны вахтеру (такие требования встречаются в некоторых организациях). Будет ли кто-нибудь следовать этому предписанию? Как это проконтролировать? К чему это приведет с точки зрения имиджа фирмы? Ясно, что это требование нежизнеспособное. Другое дело, что можно запретить использование на территории мобильных телефонов сотрудникам фирмы, при условии достаточного количества стационарных телефонов.

Принцип разумной достаточности означает, что затраты на обеспечение безопасности информации должны быть никак не больше, чем величина потенциального ущерба от ее утраты. Анализ рисков, проведенный на этапе аудита, позволяет ранжировать эти риски по величине и защищать в первую очередь не только наиболее уязвимые, но и обрабатывающие наиболее ценную информацию участки. Если в качестве ограничений выступает суммарный бюджет системы обеспечения безопасности, то задачу распределения этого ресурса можно поставить и решить как условную задачу динамического программирования.

Особое внимание в политике безопасности надо уделить разграничению зоны ответственности между службой безопасности и IT-службой предприятия. Зачастую сотрудники службы безопасности, в силу низкой технической грамотности, не осознают важности защиты компьютерной информации. С другой стороны, IT-сотрудники, являясь "творческими" личностями, как правило, стараются игнорировать требования службы безопасности. Кардинально решить эту проблему можно было бы, введя должность CEO по информационной безопасности, которому бы подчинялись обе службы.

В политике безопасности не надо детализировать должностные обязанности каких бы то ни было сотрудников (хотя приходилось видеть и такое). Эти обязанности должны разрабатывать-ся на основе политики, но не внутри нее.

Обеспечение безопасности компьютерной информации

Дополнительное внимание в политике безопасности уделяется вопросам обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Необходимо установить, как должны быть защищены серверы, маршрутизаторы и другие устройства сети, порядок использования сменных носителей информации, их маркировки, хранения, порядок внесения изменений в программное обеспечение.

Можно привести по этому поводу следующие общие рекомендации:

- в системе должен быть администратор безопасности;

- за каждое устройство должен быть назначен ответственный за его эксплуатацию;
- системный блок компьютера надо опечатывать печатями ответственного и работника IT-службы (или службы безопасности)
- жесткие диски лучше использовать съемные, а по окончании рабочего дня убирать их в сейф;
- если нет необходимости в эксплуатации CD-ROM, дисководов, они должны быть сняты с компьютеров;
- установка любого программного обеспечения должна производиться только работником IT-службы;
- для разграничения доступа сотрудников лучше всего использовать сочетание паролей и смарт-карт (токенов). Пароли должны генерироваться администратором безопасности, выдаваться пользователю под роспись и храниться им также как и другая конфиденциальная информация;
- должно быть запрещено использование неучтенных носителей информации. На учтенных носителях выполняется маркировка, например, гриф, номер, должность и фамилия сотрудника.

Еще раз напомним о разумной достаточности и здравом смысле. Внедрение любой защиты приводит к определенным неудобствам пользователя. Однако эти неудобства не должны быть существенными, иначе человек будет игнорировать существующие правила. Например, можно потребовать завести журнал пользователя персонального компьютера, в котором он должен отмечать время начала и конца работы, характер выполняемых действий, наименование созданных файлов и т.д. Можно предусмотреть процедуру удаления файлов под две росписи в журнале, да мало ли что еще взбредет в голову! Никто и никогда не будет выполнять такие вздорные требования. Другое дело, если подготовка каких-то важных документов предусмотрена на специальном компьютере в службе безопасности. Здесь журнал учета работы пользователей будет не только уместным, но и необходимым.

Крайне внимательно надо отнестись к подключению своих информационных ресурсов к Интернету. В политике безопасности этот вопрос должен быть выделен в отдельный раздел. Подключение к Интернету обычно преследует следующие цели:

- получение информации из Интернета;
- размещение в Интернете своей информации о предоставляемых услугах, продаваемых товарах и т.д.
- организация совместной работы удаленных офисов или работников на дому.

В первых двух случаях идеальным с точки зрения безопасности было бы выделение для Интернета автономного компьютера, на котором ни в коем случае не должна храниться конфиденциальная информация. На компьютере должны быть обязательно установлены антивирусные средства защиты с актуальной базой, а также правильно настроенный Firewall. При этом особый контроль надо уделить работе на этом

компьютере со сменными носителями информации, а также перлюстрации исходящей почты. В некоторых организациях вся исходящая почта попадает вначале в руки администратора безопасности, который контролирует ее и пересылает дальше.

При необходимости организации распределенной работы сотрудников фирмы наиболее приемлемым решением являются виртуальные частные сети (VPN). В настоящее время имеется много отечественных фирм-разработчиков, представляющих также услуги по установке и настройке соответствующего программного обеспечения.

Несмотря на все принятые меры, нарушения информационной безопасности могут произойти. В политике безопасности должны быть обязательно предусмотрены меры ликвидации этих последствий, восстановления нормальной работоспособности фирмы, минимизации причиненного ущерба. Большое значение здесь имеет применение средств резервирования электропитания, вычислительных средств, данных, а также правильная организация документооборота.

Аудит безопасности

Итак, вы разработали политику безопасности, претворили ее положения в жизнь. Как теперь оценить информационную безопасность вашей фирмы? Может быть, все усилия потрачены зря? На эти вопросы поможет ответить аудит безопасности. Существуют фирмы, предоставляющие подобные услуги, и, по крайней мере, два подхода к оценке.

Первый подход - оценка безопасности на качественном уровне. Проводящий оценку эксперт высказывает свое видение состояния дел в фирме, дает рекомендации по устранению замеченных им изъянов. В таком подходе нет ничего предосудительного, однако, субъективизм все же может присутствовать. Хотелось бы иметь действительно независимую, объективную оценку информационной безопасности. Причем было бы неплохо, чтобы эту, количественную, оценку признавали и другие фирмы — ваши потенциальные партнеры. Очевидно, что для этого необходима разработка некоторого набора правил или стандарта в области безопасности информационных систем.

К счастью, почти ничего разрабатывать не надо: стандарт, позволяющий дать количественную оценку информационной безопасности, уже имеется. Речь идет о международном стандарте ISO 17799. Этот документ был принят международным институтом стандартов в конце 2002 года на основе ранее разработанного Великобританией стандарта BS7799. И хотя он пока не является общепринятым документом в нашей стране, этот стандарт не противоречит руководящим документам Гостехкомиссии и приказам ФАПСИ.

Стандарт ISO 17799 позволяет получить количественную оценку комплексной безопасности фирмы. Этот процесс настолько формализован, что существует (и продается в нашей стране) программное обеспечение, позволяющее самостоятельно выполнить оценку безопасности своей компании. Это программное обеспечение представляет собой, по существу, вопросник. Сгенерированный программой отчет высылается в адрес фирмы, имеющей полномочия на проведение сертификации на соответствие этому стандарту, и та присылает вам соответствующий знак и процент соответствия стандарту, как показано на рисунке. Этот знак компания может

разместить на своем корпоративном сайте. Трудно сказать, насколько эта процедура актуальна для российских фирм, но сам подход любопытен.

В заключении, необходимо особо подчеркнуть, что необходим постоянный и эффективный контроль над реализацией политики безопасности, потому, что все технические ухищрения в области обеспечения безопасности могут оказаться бесполезными без организации должного контроля.

Администратор безопасности – полномочный представитель (лицо или группа лиц), ответственный за обеспечение безопасности в автоматизированных системах и сетях.

Административная ответственность – вид юридической ответственности за проступки и правонарушения, не являющиеся уголовно наказуемыми.

Административное право (АП) – отрасль права, регулирующая общественные отношения в сфере государственного управления. Нормы АП определяют порядок организации и деятельности управленческого аппарата, права и обязанности должностных лиц и граждан. Юридическими источниками АП являются конституция, а также содержащие административно-правовые нормы законы, указы, положения, уставы, постановления, распоряжения, приказы и инструкции различных органов управления.

Адресование документа – разрешение на доступ к конкретному документу в виде резолюции на самом документе или специальном клапане, с указанием конкретных лиц, которым дается разрешение на ознакомление (исполнение) документа.

Анализ риска – процесс определения угроз безопасности системы и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также разработка мер защиты.

Аппаратные средства защиты – механические, электромеханические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от НСД, копирования, кражи или модификации.

Аутентификация информации – установление подлинности информации исключительно на основе внутренней

«Враждебное поглощение» – это получение контроля над финансово-хозяйственной деятельностью или активами компании-цели в условиях сопротивления со стороны руководства или ключевых участников компании-цели.

Государственное право – отрасль права, представляющая собой совокупность юридических норм, закрепляющих общественное и государственное устройство, систему, принципы организации и деятельности государственных органов, основные права и обязанности граждан.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ.

Гриф конфиденциальности – специальная отметка на носителе информации либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений,

содержащихся в их носителе, проставленные на самом носителе и/или в сопроводительной документации на него. Установлено три степени секретности сведений, составляющих гостайну, и соответствующие грифы секретности: «особой важности», «совершенно секретно» и «секретно».

Доступ к конфиденциальной информации – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную или коммерческую тайну.

Закрытые данные – данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа осуществляется системой разграничения с помощью определенных правил (паролей).

Идентификация – отождествление предметов или лиц по их характеристикам, или по документам, или путем опознавания по приметам и определение полномочий, связанных с доступом к конфиденциальной информации.

Информационная безопасность – это состояние защищенности информационных ресурсов и потоков информации компании.

Информация секретная – информация, содержащая в соответствии с Законом РФ "О государственных секретах" сведения, составляющие государственную тайну.

Коммерческая тайна – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение или утечка которых может нанести ущерб его интересам. Не могут составлять коммерческую тайну учредительные документы и устав; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности; документы о платежеспособности; сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных мест; документы об уплате налогов и обязательных платежей; сведения о загрязнении окружающей среды; сведения об участии должностных лиц предприятий в кооперативах, малых предприятиях, товариществах и т. д.

Компьютерный шпионаж – подключение к компьютерам (или их прослушивание) без согласия владельцев с целью съема или повреждения содержащихся в них секретных данных.

Контрразведка – деятельность специальных органов государства (компании) в целях борьбы против разведок других государств (компаний).

Криптография – тайнопись, система изменения информации (текста, речи) с целью сделать ее непонятной для непосвященных лиц.

Многоуровневая защита – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Мошенничество – это преступление, в результате которого его жертва добровольно передает часть своих материальных средств в какой-либо форме мошеннику.

Объект промышленного шпионажа – любые материальные и нематериальные

объекты, содержащие коммерческую тайну предприятия и представляющие какой-либо интерес для заказчика: документы, чертежи, образцы продукции, неоформленные патенты, технические проекты, информация о ценах, контрактах, поставщиках и т. д.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (т.е. каждый работодатель в отношении своих работников является оператором т.к. ведет личные дела).

Персональные данные – любая информация, относящаяся к определенному на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Полиграф (детектор лжи) – прибор, который непрерывно измеряет значения кровяного давления, частоты пульса, влажности кожи, частоту дыхания и другие физиологические переменные.

Полномочия – право пользователя или уполномоченного им субъекта осуществлять определенные процедуры над охраняемыми сведениями.

Правовая защита информации – специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Правонарушение – противоправное, виновное (умышленное или неосторожное) действие или бездействие, за которое законодательством предусмотрена административная ответственность.

Разграничение доступа – система мероприятий, обеспечивающих предоставление пользователям только той информации, которая необходима им для выполнения работы.

Санкционированный доступ к информации – доступ к информации, не нарушающий правил разграничения доступа.

Служба безопасности (СБ) – система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности деятельности компании.

Управление безопасностью – система регулярных защитных мероприятий, направленных на обеспечение безопасности в соответствии с изменяющимися условиями внутренней и внешней среды.

Шпионаж – передача, похищение, добывание или собирание с целью корыстного использования или передачи иностранному государству или его агентуре сведений, составляющих конфиденциальную тайну (государственную, военную, экономическую, промышленную, коммерческую и т. п.).

Экономическая безопасность – состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и

обеспечения стабильного функционирования компании в условиях рыночной экономики.

Экономическая разведка (в бизнесе) – информационно-аналитическая работа (добывание, обработка, получение выводной информации) по экономическим проблемам.

Литература

1. Алавердов А. Р. Управление кадровой безопасностью организации. Учебник. М., 2008.

2. Абрамов В.С. Коммерческая безопасность предприятий (теория и практика). М., 1998.

3. Абрамов В.С. Обеспечение безопасности от террористических и диверсионных актов. М., 2003.

4. Бабец О.А. Опыт военной разведки на службе в коммерческой фирме. Минск, 2003.

5. Барсуков В.С. Безопасность: технологии, средства, услуги. М., 2001.

6. Баяндин Н.И. Технологии безопасности бизнеса. М., 2002.

Бородин И.А. Основы психологии корпоративной безопасности. М., 2004.

7. Ващекин Н.П. Дзлиев М.И., Урсул А.Д. Безопасность предпринимательской деятельности. М., 2002.

8. Грунин О.А., Грунин С.О. Экономическая безопасность организации. СПб., 2002.

9. Дорожкин Н.Н. Психология манипуляций в сфере обеспечения безопасности. М., 1999.

10. Доронин А.И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности. М., 2000.

11. Казаков Н.Н. Практическое пособие по безопасности предпринимательской деятельности. М., 2001.

12. Литвиненко В.И. Бизнесмен и личная безопасность. М., 2000.

13. Литвиненко В.И. Экономическая безопасность коммерческого предприятия (практические рекомендации и справочные документы). М., 2002.

14. Логинов Е.Л. Стратегия экономической войны. М., 2005.

15. Мак-Мак В.П. Служба безопасности предприятия. М., 2003.

16. Одинцов А. А. Экономическая и информационная безопасность. Справочник. М., 2005.

17. Петров М.И. Безопасностью и персонал. Журнал «Управление персоналом». М., 2006.

18. Полукарпов В.Л. Менеджмент: анализ и основные тенденции. М., 2007.

19. Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация комплексного управления безопасностью предприятия. Самара, 2008.

20. Семкин С.Н. Проектирование систем защиты информации на объектах ее обработки. М., 2001.

21. Ярочкин В. И., Бузанова Я. В. Аудит безопасности фирмы: теория и практика. М., 2005.

22. Ярочкин В. И., Бузанова Я. В. Корпоративная разведка. М., 2008.

23. Ярочкин В. И., Бузанова Я. В. Основы безопасности бизнеса и предпринимательства. М., 2005.

Интернет-ресурсы

http://www.bre.ru/security/ – Портал, помимо статей, аналитики, нормативных документов, предоставляющий возможность поиска по базам данных (например, по базе данных адресов массовой регистрации юридических лиц).

http://www.oxpaha.ru/ – Портал интернет-газеты о безопасности.

http://www.sec.ru/ – Портал, содержащий новости, статьи, форум, обзоры ПО и технических новинок в сфере безопасности.

http://www.secnews.ru/ – Портал информационно-аналитического издания по техническим средствам и системам безопасности.

http://www.wisp.ru/ – Каталог ссылок на интернет-ресурсы по безопасности (статьи, новости, аналитика, обзоры оборудования и пр.).

Нормативно-правовые акты

1. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.).

2. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) от 30 декабря 2001 г. N 195-ФЗ (с последними изменениями и дополнениями от 01 июля 2010 г.).

3. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с последними изменениями и дополнениями от 27 июля 2010 г.).

4. Налоговый кодекс Российской Федерации (с последними изменениями и дополнениями от 08 ноября 2010 г.).

5. Уголовный кодекс РФ от 13 июня 1996 г. N 63-ФЗ (с последними изменениями и дополнениями от 04 октября 2010 г.).

6. Гражданский кодекс Российской Федерации (часть первая) (с последними изменениями и дополнениями от 24 июля 2008 г.).

7. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (с последними изменениями и дополнениями от 24 июля 2007 г.).

8. Федеральный закон от 27 июля 2004 г. N 79-ФЗ «О государственной гражданской службе Российской Федерации» (с последними изменениями и дополнениями от 29 ноября 2010 г.).

9. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации» (с последними изменениями и дополнениями от 10 января 2003 г.).

10. Приказ МВД РФ от 26 декабря 2003 г. N 1033 «Об утверждении Перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну» (с последними изменениями и дополнениями от 10 февраля 2009 г.).

11. Приказ МНС РФ от 3 марта 2003 г. N БГ-3-28/96 «Об утверждении Порядка доступа к конфиденциальной информации налоговых органов».

12. Постановление Президиума Высшего Арбитражного Суда РФ от 24 ноября 1998 г. N 3900/98.

13. Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера» (с последними изменениями и дополнениями от 23 сентября 2005 г.).

14. Постановление Правительства РФ от 8 июля 1997 г. N 835 «О первичных учетных документах».

15. Постановление Правительства РФ от 31 декабря 1997 г. N 1672 "О мерах по совершенствованию порядка и методов определения амортизационных отчислений".

16. Постановление Госкомстата РФ от 30 октября 1997 г. N 71а «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты, основных средств и нематериальных активов, материалов, малоценных и быстроизнашивающихся предметов, работ в капитальном строительстве» (с последними изменениями и дополнениями от 21 января 2003 г.).

17. Постановление Госкомстата РФ от 24 марта 1999 г. N 20 «Об утверждении Порядка применения унифицированных форм первичной учетной документации».

18. Постановление Госкомстата РФ от 21 января 2003 г. N 7 «Об утверждении унифицированных форм первичной учетной документации по учету основных средств».

19. Приказ Минфина РФ от 31 октября 2000 г. N 94н «Об утверждении Плана счетов бухгалтерского учета финансово-хозяйственной деятельности организаций и инструкции по его применению» (с последними изменениями и дополнениями от 18 сентября 2006 г.).

20. Приказ Минфина РФ от 6 мая 1999 г. N 33н «Об утверждении Положения по бухгалтерскому учету «Расходы организации» ПБУ 10/99» (с последними изменениями и дополнениями от 25 октября 2010 г.).

21. Приказ Минфина РФ от 28 ноября 2001 г. N 97н «Об утверждении Указаний об отражении в бухгалтерском учете организаций операций, связанных с осуществлением договора доверительного управления имуществом» (с последними изменениями и дополнениями от 25 октября 2010 г.).

22. Приказ Минфина РФ от 19 ноября 2002 г. N 114н «Об утверждении Положения

по бухгалтерскому учету «Учет расчетов по налогу на прибыль» ПБУ 18/02» (с последними изменениями и дополнениями от 25 октября 2010 г.).

23. Приказ Минфина РФ от 13 октября 2003 г. N 91н «Об утверждении Методических указаний по бухгалтерскому учету основных средств» (с последними изменениями и дополнениями от 25 октября 2010 г.).

24.Письмо Минфина РФ от 31 июля 2003 г. N 16-00-14/243и «О начислении амортизации по объектам основных средств некоммерческих организаций».

25. Коэффициенты для переоценки нематериальных активов и малоценных предметов бюджетных учреждений по состоянию на 01.01.2003 (утв. Госкомстатом РФ).

26. Письмо Госкомстата РФ от 6 марта 2003 г. N МС-10-23/869 «Об учете основных фондов».

27. Положение ЦБР от 5 декабря 2002 г. N 205-П «О правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории Российской Федерации» (с последними изменениями и дополнениями от 26 марта 2007 г.).

28. Коэффициенты, применяемые для переоценки основных средств и нематериальных активов бюджетных учреждений (утв. Госкомстатом РФ 27 ноября 2002 г.).

29. Распоряжение Правительства РФ от 15 ноября 2002 г. N 1611-р «О переоценке основных средств и нематериальных активов бюджетных учреждений».

30. Приказ Минфина РФ от 30 марта 2001 г. N 26н «Об утверждении Положения по бухгалтерскому учету "Учет основных средств" ПБУ 6/01» (с последними изменениями и дополнениями от 25 октября 2010 г.).

31. Приказ Минфина РФ от 29 июля 1998 г. N 34н «Об утверждении Положения по ведению бухгалтерского учета и бухгалтерской отчетности в Российской Федерации» (с последними изменениями и дополнениями от 25 октября 2010 г.).