На правах рукописи

Гужов В.В., Калюжная И.А., Тюнина Н.О., Федорова Т.Н.

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ ИННОВАЦИОННОЙ СФЕРЫ ЭКОНОМИКИ

Монография

Москва – 2007

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современная российская экономика в качестве основной характеристики имеет активное формирование и развитие рыночных отношений и институтов. Ключевую роль в этом процессе играет инновационное предпринимательство. Как показывает мировой опыт, чем больше возможностей для расширения своей деятельности у инновационного бизнеса, тем более высокими являются темпы развития национальной экономики, укрепление позиций государства на мировом конкурентном рынке. В этих условиях весьма значительным фактором является обеспечение благоприятных условий развития инновационного предпринимательства в стране, повышение конкурентоспособности высокотехнологичного бизнеса.

«Конкуренция ведет к лучшему использованию знаний и достижений. Большая часть достигнутых человеческих благ получена именно путем состязания с целью завоевания конкурентных преимуществ. Конкуренция не может функционировать среди людей, лишенных предпринимательского духа» [105, с.14].

Реалии российской экономической жизни таковы, что предприниматели в своей практической деятельности сталкиваются не только с экономическими, организационными, правовыми трудностями в процессе создания своего дела и его развития, но и негативным воздействием некоторых субъектов, зачастую носящим противоправный характер, с недобросовестной конкуренцией. Это в свою очередь, обуславливает необходимость поддержания достаточного уровня экономической безопасности инновационного предпринимательства с целью сохранения и повышения конкурентоспособности на внутреннем и мировом рынках, разработки критериев такой безопасности в настоящем актуальном и перспективном аспектах.

Значение для страны субъектов инновационной деятельности определяет соответствующие требования к обеспечению их безопасности, проведению методологических и конкретно эмпирических исследований по данной проблематике. Без осмысления механизма обеспечения безопасности функционирования хозяйствующих субъектов инновационной сферы (объектов защиты) невозможно в целом разработать концепцию инновационной развития Российской Федерации.

Под безопасностью инновационного предпринимательства следует понимать состояние защищенности субъекта предпринимательской деятельности на всех стадиях его функционирования от внешних и внутренних угроз, имеющих негативные, прежде всего экономические, а также организационные, правовые и иные последствия[52, с.9].

Главной целью экономической безопасности инновационного предприятия, как хозяйствующего субъекта, является обеспечение его устойчивого и максимально эффективного функционирования, высокого уровня конкурентоспособности. Наиболее эффективное использование всех ресурсов инновационного предприятия, обеспечивающее выполнение этой

цели, достигается при решении следующих задач по повышению экономической безопасности:

- поддержание технологической независимости, формирование высокого технического и технологического потенциала;
- обеспечение достаточной финансовой устойчивости и независимости инновационного предприятия;
- оптимизация организационной структуры, постоянное совершенствование и выполнение менеджерских функций;
- обоснованная правовая защита всех видов деятельности предприятия;
- создание защиты информационной среды предприятия, его коммерческой тайны;
- формирование условий для безопасной работы сотрудников предприятия, соблюдение их коммерческих интересов;
- техническое оснащение службы безопасности предприятия.

Обеспечение экономической безопасности инновационного предприятия – это постоянный процесс реализации составляющих безопасности. Однако, следует отметить, что выше перечисленные составляющие экономической безопасности могут быть не эффективны при недостаточном обеспечении сохранности информационной среды субъектов инновационной деятельности. На сегодняшний день успешный инновационный бизнес предполагает владение информацией о рыночной конъюнктуре, финансовом положении конкурентов, их планах, новейших разработках, тенденциях развития в конкретных областях науки и производства.

Практика деятельности хозяйствующих субъектов повседневно свидетельствует об их повышенной, по сравнению с государственными структурами, уязвимости от противоправных и иных нарушающих нормальную жизнедеятельность посягательств преступных обществ, а также отдельных лиц с целью раскрытия коммерческой тайны предприятия. Поэтому обеспечение информационной безопасности своей деятельности, сохранение конкурентных преимуществ становится жизненно важной потребностью, одним из базовых принципов функционирования субъектов инновационной деятельности.

Ряд общих вопросов криминологической безопасности данных субъектов предпринимательской деятельности нашли отражение в работах А.И. Гурова, А.И. Долговой, А.Г. Шаваева, В.И. Ярочкина, Ж. Бережье, Р. Минна и ряда других ученых и практиков.

Вопросам промышленного шпионажа, сохранности коммерческой тайны и функционирования служб безопасности инновационных фирм посвящены труды А.И. Алексеева, Р.М. Гасанова, В.С. Горячева, А.В. Жукова, Ю.Ф. Каторина, А. Вольфа, К. Савки и других авторов.

Следует отметить, что перечисленные работы лишь в обобщенном виде передают зарубежный и отечественный опыт построения политики информационной безопасности субъектов инновационной деятельности, мало затрагивая вопросы прикладного характера, ориентированные на решение проблем безопасного бизнеса инновационных предпринимателей, отсутствует

комплексная методология подхода к реализации политики информационной безопасности данных хозяйствующих субъектов. В то же время сама жизнь диктует настоятельную необходимость перехода к научным основам организации защиты субъектов инновационной деятельности с целью укрепления их положения на конкурентном рынке, что и обусловило выбор темы монографии и ее актуальность в научном и практическом плане.

Целью монографического исследования является разработка методов поддержания конкурентоспособности хозяйствующих субъектов за счет обеспечения защиты инновационной деятельности на основе реализации принципов информационной безопасности бизнеса.

Цель исследования предполагает постановку следующих задач:

проведение анализа основных направлений повышения конкурентоспособности инновационного предпринимательства в аспекте информационной защиты бизнеса;

исследование основных тенденций развития современных ситуационных подходов к обеспечению информационной безопасности российских и зарубежных субъектов инновационной деятельности;

анализ угроз безопасности инновационной деятельности в результате раскрытия коммерческой тайны и потери конкурентных преимуществ хозяйствующего субъекта;

и на этой основе:

исследовать основные категории конфиденциальной информации хозяйствующих субъектов;

выявить и обобщить качественные и количественные подходы к анализу информационных рисков инновационного предпринимательства;

провести анализ существующего на сегодняшний день инструментария в области анализа и управления информационными рисками;

осуществить исследование современных методик расчета экономической эффективности применения систем информационной защиты субъектов инновационной деятельности;

разработать аппарат описания оценки экономической эффективности системы информационной безопасности;

разработать модели изучения и исследования поведения системы защиты информации на основе методологии сценарного анализа и прогнозирования;

исследовать и обобщить основные положения политики информационной безопасности и меры ее реализации на примере субъекта инновационной деятельности, разработать формальную модель построения политики информационной безопасности;

разработать структурную модель построения службы безопасности хозяйствующего субъекта инновационного бизнеса;

определить роль мониторинга информационной безопасности в системе политики информационной безопасности субъекта инновационной деятельности.

Предметом исследований являются правовые, организационно-административные, технологические и экономические процессы

функционирования системы информационной безопасности хозяйствующих субъектов инновационного бизнеса. В качестве объекта исследования выступает информационная система хозяйствующего субъекта.

Теоретическую и методологическую основу монографии составляет системный подход в сочетании с методологией структурного анализа сложных систем, методы системного анализа и стратегического прогнозирования, элементы логического моделирования и сценарного анализа.

Научную новизну содержат следующие положения и результаты исследования:

- на основе анализа мировых тенденций развития бизнеса сделан вывод о роли информационной безопасности инновационной деятельности как приоритетном направлении повышения ее конкурентоспособности на современном этапе развития экономики;
- разработана методика определения рисков информационных систем субъектов инновационной деятельности в ситуациях, когда невозможно воспользоваться количественными характеристиками для расчета величины риска. Суть методики заключается в определении посредством экспертных оценок зависимости значения риска от определенных факторов - вероятности наступления события и ущерба от наступления данного события;
- разработана модель управления информационными рисками на основе алгоритма, отражающего последовательность и взаимодействие этапов оценки рисков и выбора защитных регуляторов;
- сформулирован методический подход к определению затрат при расчете эффективности применения системы информационной безопасности на основе сравнения показателей стоимости совокупных потенциальных потерь информации без использования системы информационной безопасности и показателя стоимости реальных потерь при ее использовании;
- разработан подход к построению методологии сценарного прогнозирования и анализа поведения системы информационной безопасности при возникновении различных угроз информационной среде субъекта инновационной деятельности, в основу которого положено выделение ключевых моментов развития ситуации посягательства на защищаемый объект и разработка качественно различных вариантов отражения атаки, а также анализ и оценка каждого из полученных вариантов и возможных последствий его реализации.

Предложенные в монографии принципы и подходы к построению системы информационной безопасности инновационных фирм позволяют:

- сформировать грамотную стратегию обеспечения собственной информационной безопасности субъектов инновационной деятельности, исходя из детального анализа направлений их деятельности и комплексных требований защиты;
- повысить скорость и качество принятия управленческих решений в области информационной защиты;

- реализовать эффективную политику информационной безопасности организации;
- сформировать собственные службы защиты информации.

Обобщения, выводы и основные положения данной работы могут быть также использованы в обучении студентов и подготовке специалистов в области информационной безопасности и инновационного менеджмента.

ГЛАВА 1. РОЛЬ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ ЗАЩИТЫ В ПОВЫШЕНИИ КОНКУРЕНТОСПОСОБНОСТИ ИННОВАЦИОННОГО ПРЕДПРИНИМАТЕЛЬСТВА

1.1. Защита информационной среды инновационного предпринимательства как приоритетное направление повышения его конкурентоспособности

Национальная конкурентоспособность выступает предметом озабоченности правительства и бизнеса в каждом государстве. И хотя до настоящего времени не существует общепринятого и бесспорного определения этого института рынка, не вызывает сомнений одно: конкурентоспособна экономика той страны, хозяйствующие субъекты которой в условиях свободной конкуренции производят товары и услуги, удовлетворяющие требованиям мирового рынка.

В экономической политике последних лет понятие конкурентоспособности иногда приравнивалось к понятию приоритетности тех или иных отраслей и видов деятельности. В итоге отдельные отрасли добивались для себя разного рода преференций, хотя приоритетными они становились не по объективным критериям, а в результате лоббистской деятельности.

Промышленная политика, нацеленная на поддержку конкурентоспособных отраслей, уже не в силах дать тот эффект, на который можно было рассчитывать несколько лет назад. Предприятия, формально относясь к определенным отраслям промышленности, диверсифицируют свою экономическую деятельность и мало соответствуют формальным наименованиям отраслей.

Наша страна располагает значительной частью ресурсного потенциала планеты, и в этом ее бесспорное преимущество. Однако из этого не вытекает автоматически конкурентоспособность нашей экономики, поскольку естественными условиями нужно уметь воспользоваться. Скажем, в настоящее время существует несколько завышенная самооценка “уникальности” российских трудовых и интеллектуальных ресурсов, а именно они дают существенный вклад в создание конкурентоспособного продукта.

Группа экспертов, представляющих бизнес, науку и высшую школу, попыталась дать общую оценку состояния и перспектив российских участников конкурентной борьбы на современных рынках. В качестве инструмента такого анализа использовалась методика определения стоимости экономического потенциала отраслей экономики методом дисконтированных доходов, разработанная аудиторско-консалтинговой компанией “ФБК”. Эта методика позволила не только оценить текущее состояние отраслевой экономики, но и спрогнозировать темпы приращения их стоимостей.

В долгосрочном периоде растущий рынок будет находиться в таких секторах экономики, как промышленность, строительство, связь, торговля и общественное питание. Средние темпы прироста валовой добавленной

стоимости в период 2005-2012 гг. составят 6,9% в год. Доля промышленности в ВВП страны к 2012 г. возрастет с нынешних 26,5% до 30,1%, строительства — с 7,2% до 7,9%, связи — с 1,8% до 3,0%, торговли и общественного питания — с 22,8% до 25,7%. В то же время средние темпы прироста валовой добавленной стоимости транспорта составят 4,3%.

Однако эти агрегированные показатели в значительной степени предопределены естественно-конкурентными преимуществами, а не эффективностью работы экономических агентов, а также системы регулирования их деятельности. А именно это в конечном счете обеспечивает успех на рынке. Поэтому требуется более детальный анализ.

Критериев, по которым необходимо определять конкурентоспособность, видится два: наличие естественно-конкурентных преимуществ и наличие положительного научно-технического задела.

По первому критерию к конкурентоспособным должны быть отнесены нефтегазовая, лесозаготовительная, алюминиевая и никель-кобальтовая отрасли промышленности. По экспорту продукции данных отраслей Россия занимает 1-2-е место в мире. Они дают подавляющую часть экспортной выручки страны.

Несмотря на удаленность основных нефтяных месторождений от экспортных терминалов, относительно низкая себестоимость добычи российской нефти обеспечивает ее высокую конкурентоспособность. Вопрос конкурентоспособности российского газа на внешних рынках неоднозначен. Он связан с перспективой выхода газодобычи в регионы с высокой себестоимостью топлива, освоения месторождений шельфовой зоны.

Алюминий как крупная статья экспорта держится на относительной дешевизне энергии, льготах по транспортным тарифам, оптимизации налогов. Высокая доля экспорта (до 80% и более) почти избавляет отрасль от НДС.

По объему валютной выручки лесозаготовительная промышленность стабильно занимает пятое-шестое место среди прочих экспортеров страны. Между тем, обладая примерно пятой частью лесных ресурсов планеты, доля России в мировом лесном экспорте лишь 2-3%. Традиционно экспортируются сырье и полуфабрикаты, а импортируется продукция углубленной переработки древесины.

Признание данных отраслей конкурентоспособными продиктовано объективными преимуществами российской экономики. Ее диверсификация и политика преодоления сырьевой зависимости не должны приводить к искусственному ограничению развития одних отраслей в пользу других.

Использование второго критерия, по которому можно выделить конкурентоспособные части экономики, представляет более сложную задачу. Практически в каждой отрасли есть научно-технические заделы, но в полной мере этому критерию отвечают лишь немногие подотрасли, а именно авиакосмическая, атомная и оборонная промышленность.

В авиакосмической промышленности реальной конкурентоспособностью обладает та ее часть, которая связана с космосом, а также военное авиастроение. Гражданское самолетостроение конкурентоспособно скорее авансом.

В атомном машиностроении российские позиции на мировом рынке действительно сильны (услуги по обогащению урана, поставке топлива для ядерных реакторов, разработке и проектированию систем атомных реакторов). Потребителями отечественных технологий в ядерной области являются США, Франция, Германия, Китай.

Значительным является экспортный потенциал отечественной оборонной промышленности. На мировом рынке вооружений Россия прочно удерживается в пятерке стран-лидеров. Однако вызывает беспокойство тот факт, что Россия специализируется главным образом на экспорте “платформ” военной техники — корпусов судов, фюзеляжей и оперения самолетов, разнообразной бронетехники. Мировые рынки этой продукции не столь перспективны по сравнению с действительно наукоемкой продукцией — вычислительной техникой, авионикой, компьютеризированными системами комплексного управления ближним боем.

Таким образом, окончательный перечень конкурентоспособных отраслей сегодня включает в себя нефтедобывающую, газовую, алюминиевую, никеле-кобальтовую, лесозаготовительную, атомную, оборонную, авиакосмическую промышленность.

Ограниченность этого перечня не означает, что в других отраслях нет конкурентоспособных производств, но их частные успехи не позволяют квалифицировать эти отрасли как конкурентоспособные. Тем не менее уже перечисленных конкурентоспособных отраслей достаточно для проведения эффективной промышленной политики. Что же касается выявления потенциально конкурентоспособных отраслей, то такая задача должна решаться принципиально по-другому.

В ее основе – поддержка start-up проектов, формирующих новые сектора экономики в различных отраслях. Лишь развитие инновационного предпринимательства и венчурного инвестирования способно на фундаментальном уровне справится с возникшей проблемой. Реально оценивая нынешнее место России в рейтинге страновой конкурентоспособности, следует признать, что у нас нет другого выбора.

С экономической точки зрения инновационное предпринимательство выполняет определенную функцию в экономическом развитии любой страны. Наиболее ярко эту функцию описал австрийский ученый Йозеф Шумпетер. Предпринимателями он назвал «хозяйствующих субъектов, функцией которых является как раз осуществление новых комбинаций» [113, с.159], то есть, предприниматели реализуют нововведения, играющие ведущую роль в развитии экономики страны, повышению ее конкурентоспособности на мировом рынке. Й. Шумпетер определяет конкурентоспособность как соперничество старого с новым, с инновациями.

Идея повышения конкурентоспособности России была включена в «Концепцию национальной безопасности Российской Федерации» в редакции от 10 января 2000г. В Концепции отмечается, что Государство должно содействовать развитию частного предпринимательства во всех сферах народного хозяйства, где это способствует росту общественного

благосостояния, прогрессу науки и образования, духовному и нравственному развитию общества, защите прав потребителей [153].

Таким образом, прослеживается четкая связь между понятиями «конкурентоспособность» и «безопасность». К примеру, в США, которые по уровню конкурентоспособности занимают первое место в мире, в 1994 г. администрацией Президента была принята «Стратегия национальной безопасности США», в которой первый из семи разделов посвящен повышению конкурентоспособности.

Р.А.Фатхутдинов в разработанной им теории конкурентоспособности предприятий предлагает пользоваться понятием «ценность» - как «нечто особенное, чем система владеет (содержит в себе), стремиться сохранить либо иметь в будущем. Конкурентоспособность предприятия зависит от конкурентного преимущества – эксклюзивной ценности, обладаемой системой и дающей ей превосходство перед конкурентами»[105, с.147]. Таким образом, любая коммерческая система заинтересована в сохранении, надежной защите этой «ценности», без которой бизнес не эффективен. Главную роль в обеспечении защиты «ценности» должна сыграть система безопасности. Исходя из вышесказанного предлагаем представить цепочку получения эффекта от «ценности», дающей конкурентное преимущество на рынке, следующим образом (рис.1):

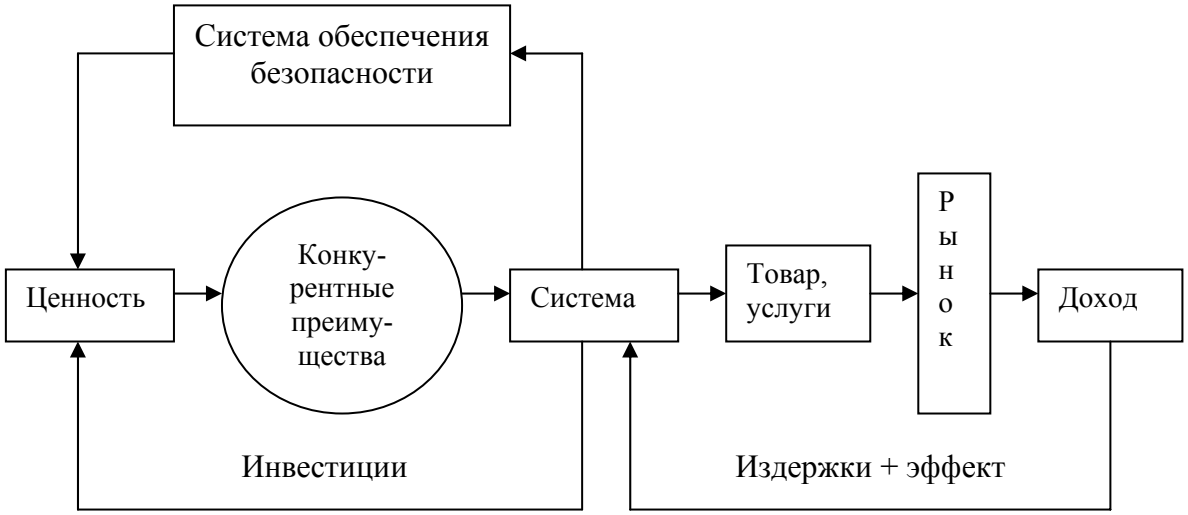

Рис.1. Цепочка получения эффекта от ценности.

Для того, чтобы грамотно построить систему безопасности субъекта инновационной предпринимательской деятельности, необходимо четко понимать и учитывать все негативные явления, представляющие угрозы «ценности» и сводящие на нет конкурентные преимущества данного субъекта.

По мнению западных теоретиков-экономистов, таких как Лезер Й. и Проэктор Д. [65, с.79], «успешное развитие инновационного предпринимательства существенно зависит от той политико-экономической среды (командно-административной или рыночно-конкурентной), в которой оно осуществляет свою деятельность». Представляется, что подобный взгляд в

области хозяйствования следует признать в качестве основополагающего фактора.

Однако не менее важным фактором, постоянно сопутствующим определенной экономической среде, является внутренняя и внешняя обстановка в стране, от которой зачастую зависит положение инновационного предпринимателя на конкурентном рынке. Современная обстановка в России характеризуется усугубляющаяся криминогенной ситуацией, появлением активно действующих структур экономической разведки, международной организованной преступности, широким применением жестких методов воздействия на субъекты предпринимательской деятельности [153].

Наличие условий, при которых создается реальная угроза причинения вреда (ущерба) хозяйствующим субъектам, снижению их конкурентоспособности ставит в ряд первоочередных и долговременных задач, требующих оперативного решения, проблему обеспечения экономической безопасности этих субъектов.

Экономическая безопасность инновационных организаций является необходимым и одним из основных принципов поддержания конкурентоспособности России на мировом рынке. Как считает О.Ю. Казакевич [50, с.201] «обеспечение безопасности хозяйствующих субъектов необходимо рассматривать в контексте становления и развития системы обеспечения экономической безопасности страны, определения ее объектов и субъектов, источников внешних и внутренних угроз безопасности, элементов, функций системы, критериев ее надежности и эффективности».

Экономическая безопасность государства – это такое состояние экономики, когда экономическое благополучие участников соответствующих общественных отношений, стабильность внутреннего рынка данной страны хотя и зависят от действия внешних факторов, но негативное влияние последних нейтрализуется резервами хозяйствующих субъектов, позволяющих сохранить стабильность экономики в целом, ее конкурентоспособность. [109, с.6]

Криминологический аспект безопасности субъектов инновационной предпринимательской деятельности – неотъемлемая часть общей системы национальной экономической безопасности. С криминологической точки зрения негосударственные хозяйствующие субъекты могут быть дифференцированы по критерию уровня виктимизации. Эта проблема подробно рассматривается в научных трудах О.Б. Малежина [71]. Уровень криминологической виктимизации характеризуется отношением числа потерпевших от преступлений к общей численности обследуемой социальной группы. По данным проведенных исследований, средний уровень виктимизации субъектов предпринимательской деятельности соответственно составил:

- В сфере индивидуального предпринимательства - 61%;
- В сфере малого бизнеса - 57 %;
- В сфере среднего бизнеса - 29%;
- В сфере большого (крупного бизнеса) - 14%.

Таким образом, среди рассмотренных групп наиболее подверженными криминальным угрозам являются лица, занимающиеся индивидуальным предпринимательством и коммерческие фирмы, функционирующие в сфере малого бизнеса, составляющие значительную часть инновационного сектора экономики. Наименее уязвимые представители крупного бизнеса - несколько ниже среднего уровня виктимизации.

Постановка вопроса о концептуальных основах обеспечения криминологической безопасности субъектов предпринимательской деятельности объективно необходима еще и потому, что комплексная разработка этого аспекта функциональной деятельности указанных структур на фундаментальном уровне еще не осуществлялась.

В исследованиях отечественных и зарубежных ученых рассмотрены отдельные вопросы по затрагиваемой проблеме. Так, феномен организованной и иной преступности в сфере экономики, основные закономерности, содержание и динамика этого явления достаточно подробно исследованы в работах А.И. Гурова, А.И. Долговой, А.Г. Шаваева, В.И. Ярочкина и ряда других ученых и практиков [41, 44, 45, 109, 117]. В числе зарубежных ученых и публицистов, уделивших внимание данной проблеме следует особо отметить работы Ж. Бережье, Р. Минна [30, 74].

С учетом сложившейся политической и экономической ситуации в России сформировался интерес к проблемам обеспечения защиты субъектов инновационного предпринимательства от посягательств со стороны организованной преступности, промышленного шпионажа и иных правонарушений, сохранности коммерческой тайны. Хотя эти исследования представлены сравнительно широко, следует специально выделить работы А.И. Алексеева, Р.М. Гасанова, В.С. Горячева, А.В. Жукова, Ю.Ф. Каторина, В.И. Ярочкина. [25, 35, 38, 47, 52, 115]

Исследование проблемы показывает, что все факторы, способствующие преступным посягательствам на безопасность инновационного предпринимательства, условно могут быть разделены на внутренние и внешние.

В числе основных внутренних криминогенных факторов, позволяющих выделить субъекты инновационного предпринимательства среди иных объектов защиты в интересах задействования всех сил и средств такой защиты, следует отметить:

- наличие у данных субъектов заказов, связанных с созданием в России новейших образцов техники и технологий, фундаментальных и прикладных научных исследований, опережающих мировой уровень;
- их участие этих фирм в продвижении на мировой рынок высокотехнологических товаров;
- уровень угроз для экономики отрасли, региона, государства, определяемый вынужденной остановкой или сбоями в функционировании субъектов предпринимательской деятельности;
- повышенная экологическая опасность, связанная с деятельностью этих субъектов.

К факторам, составляющим внешние угрозы криминологической безопасности хозяйствующих субъектов, относятся:

- формирования организованной преступности;
- негосударственные организации и отдельные лица, специализирующиеся на проведении промышленного шпионажа;
- деятельность спецслужб иностранных государств, ставящие своей целью добывание информации по экономической проблематике.

Как отмечает Р.М. Гасанов, экономический шпионаж как сфера тайной деятельности по сбору, анализу, хранению и использованию особо ценной конфиденциальной информации охватывает все сферы рыночной экономики [35, с.6].

В основе причинной обусловленности возникновения, развития и дальнейшего совершенствования такого явления, как экономическая разведка, лежит обеспечение конкурентных преимуществ – либо национальных, либо корпоративных.

В условиях продолжающегося воздействия на состояние всемирного хозяйства и его подсистем разноуровневых глобальных факторов, а именно: технологической революции, обострения энергосырьевой проблемы, кризиса мировой финансово-кредитной системы, усиление взаимозависимости национальных хозяйств, их экономической политики, сближения экономических уровней развития различных стран; преодоления межсистемных противоречий между странами, проявляющегося в признании конкуренции как главного фактора, обеспечивающего равновесие внутрихозяйственного развития, несомненно, экономическая разведка сохранит свою актуальность и в дальнейшем. Следует отметить, главное предназначение разведки – добывание информации.

В своем исследовании Е.Степанов [99, с.49] приходит к выводу, что прочность положения фирмы в значительной степени зависит от владения информацией о результатах перспективных исследований и разработок, рыночной конъюнктуре, финансовом положении конкурентов, тенденциях развития в конкретных областях бизнеса, получить которую и должна экономическая разведка. Она также способствует выявлению уязвимых мест и недостатков в системе безопасности компании, что позволяет разрабатывать адекватные меры защиты от промышленного шпионажа, мошенничества и других угроз.

Информация и бизнес на сегодняшний день являются взаимосвязанными понятиями. Стремительное развитие информационных технологий привело к созданию и быстрому росту глобальной сети Internet, формированию информационной среды, оказывающей влияние на все сферы предпринимательской деятельности. Новые технологические возможности облегчают распространение информации, повышают эффективность производственных процессов, способствуют расширению деловых операций в сфере бизнеса. Эффективность бизнеса субъекта предпринимательской деятельности напрямую зависит от качества и оперативности управления бизнес-процессами.

Предприятия нового типа – это разветвленная сеть распределенных подразделений, филиалов и групп, взаимодействующих друг с другом. Распределенные корпоративные информационные системы становятся сегодня важнейшим средством производства современной компании, они позволяют преобразовать традиционные формы бизнеса в электронный бизнес. Электронный бизнес использует глобальную сеть Internet и современные информационные технологии для повышения эффективности всех сторон деловых отношений, включая продажи, маркетинг, платежи, финансовый анализ, поддержку клиентов и партнерских отношений.

Важнейшее условие существования электронного бизнеса в инновационном предпринимательстве – его информационная безопасность. А.В. Соколов и В.Ф. Шаньгин [96, с.16] определяют информационную безопасность, как «защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий, которые могут нанести ущерб владельцам или пользователям информации». Информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей, в этом состоит ее конфиденциальность. В своем научном труде А.В. Петраков [82, с.49-53] анализирует понятие конфиденциальности и дает определение конфиденциальной информации и данным, как «статусу определяющему степень их защиты». Разрушение информационного ресурса, его временная недоступность или несанкционированное использование (т.е. нарушение установленных правил доступа и использования информации) могут нанести хозяйствующему субъекту значительный материальный ущерб и даже привести к полному закрытию компании.

Без должной степени защиты информации внедрение информационных технологий может оказаться экономически невыгодным в результате значительного ущерба из-за потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях.

Корпоративные сети и системы, внедряемые на субъектах предпринимательской деятельности, объективно приводят к росту стоимости информации, хранящейся и обрабатываемой в них. Информация приобретает для предпринимателей особую ценность, дает хозяйствующему субъекту конкурентные преимущества по отношению к другим участникам рынка. Реализация решений, обеспечивающих безопасность информационных ресурсов в предпринимательской деятельности, повышает эффективность всего процесса информатизации на фирме, обеспечивая сохранность дорогостоящей деловой информации, циркулирующей в локальных и глобальной информационных средах.

Поддержание массовых и разнообразных связей предприятия через Internet с одновременным обеспечением безопасности этих коммуникаций является сегодня основным фактором, влияющим на развитие корпоративной информационной системы коммерческой фирмы. Следует отметить, что средства взлома компьютерных сетей и хищения информации развиваются так же быстро, как и все высокотехнологичные компьютерные отрасли. В этих

условиях обеспечение информационной безопасности КИС является приоритетной задачей для руководителей хозяйствующих субъектов, поскольку от сохранности корпоративных информационных ресурсов во многом зависит качество и оперативность принятия стратегических решений и эффективность их реализации, что в конечном итоге отражается на конкурентоспособности субъектов предпринимательской деятельности.

Задача обеспечения информационной безопасности КИС хозяйствующего субъекта традиционно решается построением системы информационной безопасности (СИБ), определяющим требованием к которой является сохранение вложенных в построение КИС инвестиций. Для того чтобы обеспечить надежную защиту ресурсов корпоративной информационной системы в подсистеме информационной безопасности должны быть реализованы самые прогрессивные и перспективные технологии информационной защиты. Особое внимание уделяется комплексному подходу к обеспечению информационной безопасности, предполагающему рациональное сочетание методов, технологий и средств информационной защиты, эффективное применение правовых, программно-технических и организационных мер. По данным аналитических исследований, приведенных в совместной работе Ю.Ф. Каторина, Е.В. Куренкова, А.В. Лысова и А.Н. Остапенко [52, с.78], удельный вес каждого из перечисленных компонентов соответственно составляет:

- правовые методы – 60%;
- программно-технические – 30%;
- организационные методы – 10%.

Из приведенных цифр наглядно видно, что правовые методы занимают лидирующее место по своей значимости, и именно поэтому правовое обеспечение рассматривается как приоритетное направление в политике обеспечения информационной безопасности инновационного предпринимательства.

Нормативно-правовая база информационной защиты включает в себя различные федеральные законы, акты и методические документы, направленные на построение системы информационной безопасности, регламентирующие порядок защиты конфиденциальной информации и информационные отношения в области предпринимательства в целом, такие как: Федеральный закон от 20.02.95г. №24-ФЗ "Об информации, информатизации и защите информации", Федеральный закон от 04.07.96 г. №85-ФЗ "Об участии в международном информационном обмене", Указ Президента Российской Федерации от 06.03.97 г. № 188 "Перечень сведений конфиденциального характера", Постановление Правительства Российской Федерации от 03.11.94 г. №1233 "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органов исполнительной власти", а также другие нормативные правовые акты и ГОСТы по реализации мер защиты информации (приложение 1).

В РФ вопросам информационной безопасности уделяется приоритетное направление. Доказательством этому служит утверждение в сентябре 2000 г.

Доктрины информационной безопасности Российской Федерации, которая особо подчеркивает жизненную важность этих вопросов для государства, общества и предпринимательской сферы в частности [9].

Подводя итог анализу литературных источников по данной проблематике, можно сделать вывод, что успешное развитие предпринимательской деятельности, повышение ее конкурентоспособности во многом зависит от наличия конкурентных преимуществ, выраженных в эксклюзивной ценности. В связи с этим, хозяйствующие субъекты серьезно заинтересованы в сохранении этой ценности. Данная задача решается посредством построения системы обеспечения экономической безопасности. Учитывая бурное развитие информационных технологий на современном этапе, возрастание роли информации во всех бизнес-процессах, преобразование традиционных форм бизнеса в электронный бизнес, логично предположить, что эксклюзивная ценность, дающая конкурентные преимущества предпринимательским структурам. Поэтому предлагаем рассматривать вопросы разработки методов и механизмов обеспечения конкурентоспособности хозяйствующих субъектов за счет обеспечения безопасности их деятельности и защиты конкурентных преимуществ на основе реализации принципов информационной безопасности инновационного бизнеса.

Основываясь на проведенном анализе литературы, считаем, что функционирование системы экономической безопасности в целях обеспечения конкурентоспособности инновационного предпринимательства, рассматриваемое в аспекте защиты информационной среды субъектов предпринимательской деятельности, должно основываться на четырех уровнях:

- Первый – соблюдение политико-правовых международных условий существования субъектов инновационного предпринимательства в рамках государства, обеспечивающих возможность свободного выбора и осуществления стратегических задач инновационного развития (не подвергаясь при этом внешнему политическому, экономическому и иному давлению, вмешательству во внутренние дела), использования результатов научно-технической революции и международного экономического сообщества в интересах развития экономики страны на основе взаимовыгодного сотрудничества и повышения конкурентоспособности российских субъектов предпринимательской деятельности на мировом рынке.
- Второй – обеспечение достижимости макроэкономических целей на федеральном и региональном уровнях путем создания внутригосударственной подсистемы экономической безопасности, предусматривающей прежде всего своевременное выявление и подавление, либо нейтрализацию источников внешней и внутренней угрозы безопасности инновационной деятельности, защиту от недобросовестной конкуренции и промышленного шпионажа.
- Третий – объектовая защита субъектов инновационного предпринимательства от противоправных посягательств конкурентов в основном с использованием сил и средств самих объектов защиты.
- Четвертый – непосредственно защита конфиденциальной информации и коммерческой тайны, сохранение конкурентных преимуществ, как

важнейшее условие развития, устойчивости и эффективности инновационной деятельности, осуществляемая путем построения подсистем информационной безопасности хозяйствующего субъекта.

Все уровни системы обеспечения экономической безопасности не изолированы друг от друга и находятся в неразрывном единстве, предполагающем правильное определение стратегических целей и задач обеспечения защиты экономической деятельности хозяйствующего субъекта, применение апробированной с учетом мирового опыта и российской специфики тактики достижения решения поставленной задачи, а также взаимодополнение и взаимоподдержку при сохранении централизованной координации.

Вместе с тем анализ специальной литературы по рассматриваемой проблематике, а также практический анализ работы ряда предприятий инновационного бизнеса дает основание сделать вывод о том, что до настоящего времени не сложилась единая точка зрения по вопросам комплексного, системного подхода к обеспечению безопасности субъектов инновационного предпринимательства, механизма и принципов создания и функционирования служб безопасности таких субъектов, их взаимодействия между собой и правоохранительными органами. У значительного числа руководителей хозяйствующих субъектов еще не сформировалось понимание приоритетности обеспечения информационной безопасности как одного из базовых принципов эффективной экономической деятельности, поддержанию ее конкурентоспособности. В силу этого на практике задача обеспечения экономической безопасности хозяйствующего субъекта с точки зрения защиты его информационной среды нередко относится к второстепенной, либо не ставится вообще.

Указанные обстоятельства позволяют утверждать, что современное состояние разработанности проблемы обеспечения безопасности инновационных организаций не отвечает в должной мере потребностям эффективной и надежной защиты таких субъектов от источников внешних и внутренних угроз безопасности, выработке оптимальных экономических решений в сфере формирования национальной инновационной системы.

Это обстоятельство в ближайшем будущем может привести к экономическим потерям в сфере инновационного предпринимательства, значительно ослабить их конкурентоспособность на отечественном и зарубежных рынках.

1.2. Современные тенденции в области информационной защиты инновационного предпринимательства

Анализ современного состояния экономической безопасности инновационного предпринимательства в аспекте защиты информационной среды российских и зарубежных субъектов инновационной деятельности, включенных в содержание данной части работы, осуществлялся на основе ранее предложенного понятия (п.1.1.) успешного функционирования четырех–уровневой системы защиты экономической деятельности хозяйствовующих

субъектов с целью повышению их конкурентоспособности на национальном и мировом рынках.

Создание политико-правовых международных условий существования и развития субъектов инновационного предпринимательства и обеспечение их безопасности на федеральном и региональном уровнях регламентируются нормативно-правовыми базами государств, включающими различные федеральные законы и акты, а также международными соглашениями и стандартами.

Сегодня в России и за рубежом наблюдается значительный рост интереса к проблемам информационной безопасности, который объясняется бурным развитием крупномасштабных распределенных информационных систем и значительным ущербом, который наносится компьютерными преступлениями.

По официальным источникам, ежегодные потери только делового сектора США от незаконного проникновения в информационные корпоративные системы составляют от 150 до 300 млн.долл. Средний ущерб от одного компьютерного преступления США составляет 450 тыс.долл., а максимальный – 1 млрд.долл.

В Великобритании ежегодные потери составляют 2.5 млрд.фунтов стерлингов, а в странах Западной Европы – 30 млрд.долл [62, с.56].

Статистика компьютерных преступлений, совершенных в России в последнее время, достаточно впечатляюща и наглядна, и далеко не все случаи официально зафиксированы. И если (по данным Главного информационного центра МВД РФ) еще несколько лет тому назад доля явных компьютерных преступлений от общего числа в кредитно-финансовой сфере бизнеса составляла не более 2%, что в абсолютных цифрах насчитывало около сотни [100, с.16], то, например, в 2006 году по данным Управления «Р» зафиксировано 1375 компьютерных преступлений, а ущерб от одного компьютерного преступления составляет в среднем 300-500 тысяч рублей, а в отдельных случаях и значительно больше [84, с.38].

Международный опыт уголовно-правовой классификации компьютерных преступлений, накопленный в ряде ведущих высокотехнологичных стран мира, позволил сформировать так называемые «Минимальный список нарушений» и «Необязательный список нарушений». В приложении 2 приводятся основные перечни компьютерных преступлений, содержащиеся в этих списках. Данные списки были разработаны государствами-участниками Европейского сообщества и официально оформлены как «Руководство Интерпола по компьютерной преступности» [62, с.116].

В России большая часть преступлений, посягающих на экономическую, в том числе и информационную безопасность хозяйствующих субъектов впервые криминализована в новом УК РФ [3].

До 1 января 1997 года – даты вступления в действие нового Уголовного Кодекса Российской Федерации (УК РФ) в России отсутствовала возможность эффективно бороться с посягательствами на информационную безопасность субъектов предпринимательства, в частности с компьютерными преступлениями и нарушениями. Несмотря на явную опасность для

отечественного бизнеса, данные посягательства не были противозаконными, то есть они не упоминались российским уголовным законодательством. Хотя еще до принятия нового УК в России была осознана необходимость правовой борьбы с компьютерными преступлениями.

Сегодня составы компьютерных преступлений приведены в главе 28 УК РФ, которая называется «Преступления в сфере компьютерной информации» и содержит три статьи: «Неправомерный доступ к компьютерной информации» (ст.272), «Создание, использование и распространение вредоносных программ ЭВМ» (ст.273) и «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» (ст.274).

В большинстве стран соответствующие нормы сильно рассредоточены по соответствующим УК либо даже по разным законам, так что помещение их в одну главу было несомненным успехом российских законодателей. В то же время следует заметить, что, например, американское законодательство более конкретно [73], четкое руководство к действию в случае нарушения компьютерной безопасности отражено в части 18 Свода законов.

Имеющиеся в России законы и указы [7, 10] носят в основном запретительный характер. В то же время следует учитывать, что в данном случае от государства требуется в первую очередь поддержка, организация и координация работ. В других странах это поняли довольно давно. Так, в США в 1987 году был принят закон о компьютерной безопасности (Computer Security Act, вступил в силу в сентябре 1988 года). Этот закон предусматривает комплекс мер по обучению пользователей, имеющих дело с критичной информацией, по подготовке разъяснительных руководств и т.д., без чего сознательное поддержание режима информационной безопасности просто невозможно. И данный закон на самом деле выполняется [142].

Характеризуя в целом текущее состояние отечественного нормативно-правового обеспечения информационной безопасности, можно отметить, что сложность компьютерной техники, неоднозначность квалификации, трудность сбора доказательной информации, а также неохваченность полностью всех видов компьютерных преступлений и нарушений пока в полной мере не позволяют эффективно бороться с данными проявлениями. Тем не менее, позитивность произошедших перемен в российском правовом поле очевидна.

Стремительное внедрение и развитие технологий Internet во всем мире сегодня затрагивает все основные сферы бизнеса. Корпоративные системы, соединенные с помощью открытых каналов связи в единую глобальную сеть, становятся прекрасными мишенями для проведения различных атак, являются уязвимыми для разного рода злоумышленников и в целом представляют возможность проведения самых настоящих электронных диверсий и информационных войн. Бывший директор ЦРУ Джон Дейч поставил электронную угрозу, ввиду ее значимости, в один ряд с такими страшными угрозами, как ядерная, химическая и бактериологическая [84, с.18].

Последнее обстоятельство выводит вопросы информационной безопасности на первое место среди приоритетных направлений совершенствования всей системы национальной безопасности государств.

После трагических событий 11 сентября 2001г. президент Буш подписал указ №13231, специально посвященный вопросам информационной безопасности страны – «Защита критической инфраструктуры в информационный век» [136].

О серьезности отношения к вопросу информационной безопасности в России говорит утверждение Президентом РФ в сентябре 2000 г. Доктрины информационной безопасности Российской Федерации, закладывающей основы информационной политики государства. С учетом существующих угроз для защиты национальных интересов России государство планирует активно развивать отечественную индустрию средств информации с последующим выходом продукции на мировой рынок, обеспечивать гарантии безопасности для национальных информационных систем.

Анализ развития нормативной базы оценки безопасности информационных технологий (ИТ) позволяет понять мотивационные посылки, которые привели к созданию современных международных стандартов.

Прежде всего это связано с коренными изменениями окружающей среды бизнеса. В 80-е годы прошлого столетия утвердилась интернационализация экономики, которой было присуще взаимопроникновение и взаимозависимость между экономиками отдельных стран, а в 90-е годы началась ее глобализация – новый и качественно иной этап, ведущий к созданию единого мирового рынка.

В 1983 году в качестве стандарта оценки безопасности компьютерных систем в США был принят стандарт TCSEC, известный также под названием «Оранжевая книга», который определил требования к средствам защиты информации, которые должны быть включены в компьютерную систему, предназначенную для обработки критичной информации. Следуя по пути интеграции, Европейские страны (Франция, Германия, Великобритания и Нидерланды) в 1991 году приняли согласованные «Критерии оценки безопасности ИТ» (ITSEC). Основное отличие «Европейских критериев» от «Оранжевой книги» заключалось в обращении значительно большего внимания на вопросы гарантированности безопасности информационных технологий, затрагивающей два аспекта – эффективность и корректность средств обеспечения безопасности. Также были разработаны «Канадские критерии» (CTCPEC), которые в отличии от «Оранжевой книги» были изначально нацелены на широкий диапазон компьютерных систем [84].

В 1990 году под эгидой Международной организации по стандартизации (ИСО) были развернуты работы по созданию международного стандарта в области оценки безопасности информационных технологий. Разработка этого стандарта преследовала следующие цели:

- унификация национальных стандартов в области оценки безопасности ИТ;
- повышения уровня доверия к оценке безопасности ИТ;
- сокращения затрат на оценку безопасности ИТ;
- сокращение затрат на оценку безопасности ИТ на основе взаимного признания сертификатов.

Новые критерии получили название «Общие критерии оценки безопасности информационных технологий» (ОК) и были призваны обеспечить взаимное признание результатов стандартизованной оценки безопасности на

мировом рынке ИТ. ОК обобщили содержание и опыт использования «Оранжевой книги», развили положения «Европейских критериев».

Как показывают оценки специалистов в области информационной безопасности, таких как, Д.П. Зегжда, А.М. Ивашко [48], В.В. Липаев [66], М.Т. Кобзарь, И.А. Клайда, А.П. Трубачев [55, 56] по уровню систематизации, полноте и возможностям детализации требований, универсальности и гибкости в применении «Общие критерии» представляют наиболее совершенный из существующих в настоящее время стандартов.

Целесообразность использования основных положений и конструкций ОК при разработке комплекса нормативных документов, методического и инструментального обеспечения оценки безопасности ИТ была осознана в России, первоочередным шагом в этом направлении является принятие российского стандарта ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» [140].

Следует отметить, что до настоящего времени в России и других странах, развитие систем защиты современных информационных технологий отстает от бурных темпов создания собственно этих технологий. Как пример, можно привести важнейшее средство защиты информации от искажения – эклектронно-цифровую подпись (ЭЦП). Внедрение средств ЭЦП, например, в банковские электронные технологии произошло намного позже создания и развертывания самих этих технологий. Федеральный закон «Об электронной цифровой подписи» был разработан и принят лишь в январе 2002г., с 1 июля 2002 года принята и введена в действие новая версия стандарта ЭЦП ГОСТ РЗИ.10-01, по своим характеристикам существенно превосходящая предыдущий стандарт.

В настоящее время отечественные компании в своей деятельности в области защиты конфиденциальной информации все чаще обращаются к практике адаптации к российским условиям и применению методик международных стандартов (ISO 17799, BSI и пр.).

На современном этапе в России мощный импульс в сфере ИТ-технологий, который дала Федеральная программа «Электронная Россия», постепенно переводит общество на более высокий технологический уровень, где ключевое значение имеет информация. Успешное функционирование хозяйствующих субъектов, поддержание их конкурентоспособности, как было отмечено в п.1.1., невозможно без защиты их информационных ресурсов. Грамотная стратегия использования защиты информации для поддержки и развития бизнеса сегодня является одним из ключевых факторов обеспечения конкурентоспособности компании на рынке. В последнее время на российском рынке информационной безопасности наблюдалась положительная динамика роста объема продаж аппаратно-программных средств защиты конфиденциальной информации, а также услуг в области консалтинга и аудита информационной безопасности (рис.2) [85].

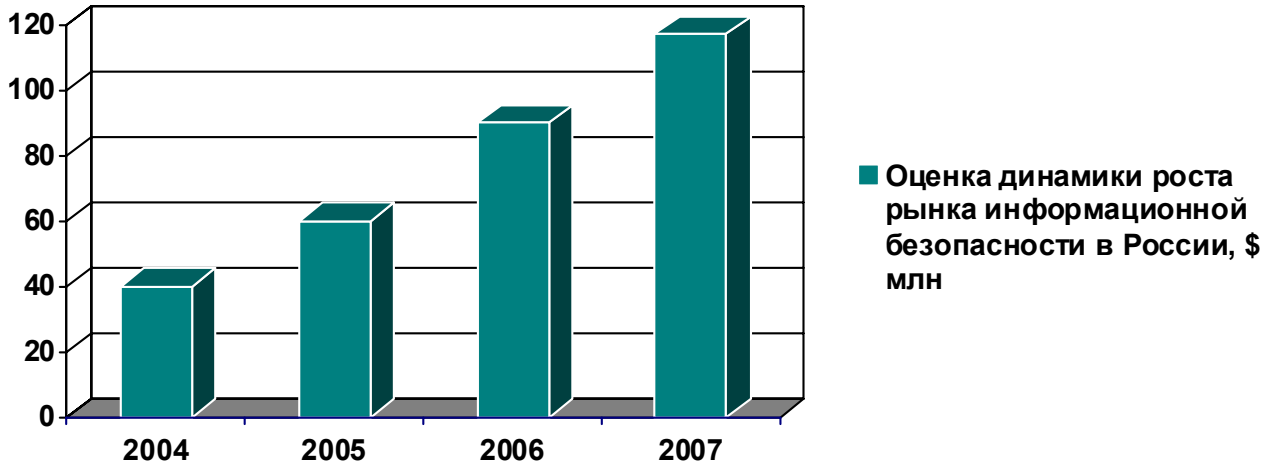

Рис.2. Динамика рынка информационной безопасности.

Отмеченные тенденции развития рынка информационной защиты и проблемы роста отечественных компаний, связанные с постоянной реструктуризацией и модернизацией производства и сбыта, заставляют российских предпринимателей заново переосмыслить стратегию и тактику существующих корпоративных систем защиты информации, разрабатывать и совершенствовать подходы к реализации этой защиты. Существенную помощь предпринимательским структурам в этом направлении оказывают фирмы, специализирующиеся в области защиты информации. Таблица 1 отражает динамику основных направлений на рынке информационной безопасности. [Данные предоставлены сотрудниками ООО ИК «Сибинтек»].

Таблица 1.

Динамика основных направлений информационной безопасности

	Доля рынка	Прогнозируемый ежегодный рост рынка
Продукты и решения	80%	50%
Консалтинговые услуги в области ИБ	20%	100-150%

В связи с этим в настоящее время ряд ведущих отечественных компаний осознали преимущество дополнительных собственных инициатив, направленных на обеспечение устойчивости функционирования корпоративных информационных систем и поддержания непрерывности бизнеса в целом, некоторые компании уже приняли собственные Концепции ИБ.

Так например, по данным Cnews, российская компания «Информзащита», работающая в сфере информационных технологий, является первой по росту оборота, с показателем в 226% (при составлении рейтинга рассматривались компании с оборотом не менее 100 млн. рублей в год) [152]. И это не случайно – наряду с активным внедрением ИТ, не менее интенсивно в этой компании

развивается сегмент IT-Security. Именно тот, кто решает проблему развития и конкурентоспособности в комплексе с информационной безопасностью и становится победителем.

Среди основных тенденций в области информационной безопасности, наблюдаемых в деятельности ведущих отечественных компаний, особо можно отметить:

- Уход от решения локальных задач в сторону построения комплексных систем информационной безопасности;
- Возрастание роли организационно-управленческих мер обеспечения безопасности;
- Создание системы ИБ начинается с определения концепции и политики компании в области информационной безопасности;
- Все большее значение приобретают вопросы тестирования и мониторинга состояния системы информационной безопасности;
- При оценке эффективности работы систем информационной безопасности все чаще применяются экономические показатели [72].

В условиях ожесточенной конкурентной борьбы на международном и отечественном рынке, когда масштабы промышленного шпионажа резко возрастают, традиционные подходы к обеспечению экономической безопасности инновационного предпринимательства, базирующиеся на пассивной защите, требуют значительных ресурсов и не могут принципиально обеспечить требуемого уровня. В силу этого в последние несколько лет активно развиваются адаптивные системы защиты, обеспечивающие активное противодействие злоумышленникам.

Исходя из фундаментальных положений разработанной В.А. Герасименко [36] общей концепции защиты информации наиболее перспективной является упреждающая концепция. Основная идея которой заключается в принятии превентивных мер к поддержанию безопасности информации. Этот подход основан на анализе возможных угроз информационной системе, поиске уязвимостей, которые могут быть использованы для реализации атаки, и разработке соответствующих контрмер [67, с. 29].

Проанализировав основные мировые тенденции в области экономической безопасности применения информационных технологий, можно отметить, что в настоящее время повседневная деятельность большинства хозяйствующих субъектов во многом зависит от информационных систем. Поэтому грамотная стратегия обеспечения безопасности этих систем для поддержки и развития бизнеса сегодня является одним из ключевых факторов обеспечения конкурентоспособности субъектов предпринимательской деятельности как на внутреннем национальном, так и на мировом рынке. Сегодня понятие «обеспечение безопасности информационной системы» становится синонимом бесперебойного и устойчивого функционирования бизнеса в целом, его высокой конкурентоспособности.

Наметившиеся тенденции развития отечественного рынка информационной безопасности позволяют сделать вывод о необходимости

внедрения стратегии адаптации к российским условиям и применении на практике методик международных стандартов, а также использование внутренних корпоративных методик и разработок, что несомненно выведет на качественно новый уровень эффективность экономической безопасности российского бизнеса. Наличие развитой системы информационной безопасности гарантирует жизнеспособность и конкурентоспособность любого субъекта предпринимательской деятельности.

1.3. Сущность и классификация признаков угроз конфиденциальности для обеспечения конкурентных преимуществ субъектов инновационного предпринимательства.

Предпринимательская деятельность во всех сферах неразрывно связана с получением и использованием различного рода информации. Причем в современных условиях информация представляет собой особого рода товар, имеющий определенную ценность, дающую конкурентные преимущества хозяйствующим субъектам. Для предпринимателя зачастую наиболее ценной является информация, которую он использует для достижения целей фирмы и разглашение которой может лишить его возможностей реализовать эти цели, то есть, создает реальные угрозы безопасности предпринимательской деятельности. Безусловно, не вся информация может, в случае ее разглашения, создавать эти угрозы, однако существует определенная ее часть, имеющая особую ценность для субъекта предпринимательской деятельности, которая нуждается в защите.

Информация, используемая в инновационном предпринимательстве, деятельности весьма разнообразна. Ее можно разделить на два вида [87]: промышленная и коммерческая.

К промышленной относится информация о технологии и способе производства, технических открытиях и изобретениях, “ноу-хау”, конструкторская документация, программное обеспечение и т.п. Коммерческая информация – это информация о финансово-экономическом положении предприятия (бухгалтерская отчетность), кредитах и банковских операциях, о заключаемых договорах и контрагентах, структуре капиталов и планах инвестиций, стратегических планах маркетинга, анализе конкурентоспособности собственной продукции, клиентах, планах производственного развития, деловой переписке и пр.

Вся эта информация представляет различную ценность для самого предпринимателя и, соответственно, ее разглашение может привести (либо не привести) к угрозам информационной безопасности различной степени тяжести, даже к потере конкурентоспособности коммерческой фирмы. Поэтому информацию, используемую в процессе предпринимательской деятельности, специалисты по информационной защите - А.В. Жуков, И.Н. Маркин, В.Б. Денисов [47] предлагают разделить на три группы:

- информация для открытого пользования любым потребителем в любой форме;

- информация ограниченного доступа – только для органов, имеющих соответствующие законодательно установленные права (милиция, налоговая полиция, прокуратура);
- информация только для работников (либо руководителей) фирмы.

Эта классификация представляется наиболее удобной в практическом плане и используется во хозяйствующих субъектах.

Информация, относящаяся ко второй и третьей группам является конфиденциальной и имеет ограничения в распространении. Конфиденциальная информация – это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ [7, 8, 9, 11, 13].

В соответствии со «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации» (СТР-К) [20] дано определение конфиденциальной информации как информации «с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным, содержащейся в государственных (муниципальных) информационных ресурсах, накопленной за счет государственного (муниципального) бюджета и являющейся собственностью государства (к ней может быть отнесена информация, составляющая служебную тайну и другие виды тайн в соответствии с законодательством Российской Федерации, а также сведения конфиденциального характера в соответствии с "Перечнем сведений конфиденциального характера", утвержденного Указом Президента Российской Федерации от 06.03.97 №188), защита которой осуществляется в интересах государства, а также информации о фактах, событиях и обстоятельствах частной жизни граждан, позволяющей идентифицировать личность (персональные данные)».

Наряду с конфиденциальностью важными категориями информации являются также ее целостность, то есть, гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений, таких как ее уничтожение или модификация, и доступность, то есть гарантия обеспечения своевременного и беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия [97].

Говоря о безопасности информации с ограниченным доступом необходимо определить не только основные требования, но и классифицировать угрозы, результатом реализации которых может быть:

- утечка информации (извлечение, копирование, подслушивание);
- нарушение целостности (модификация, т.е. подделка, изменение содержания или объема информации, и уничтожение данных);
- блокирование информации (невозможность доступа к данным).

Классификацию основных требований и угроз конфиденциальной информации представляется наиболее наглядно представить в виде схемы (рис.3).

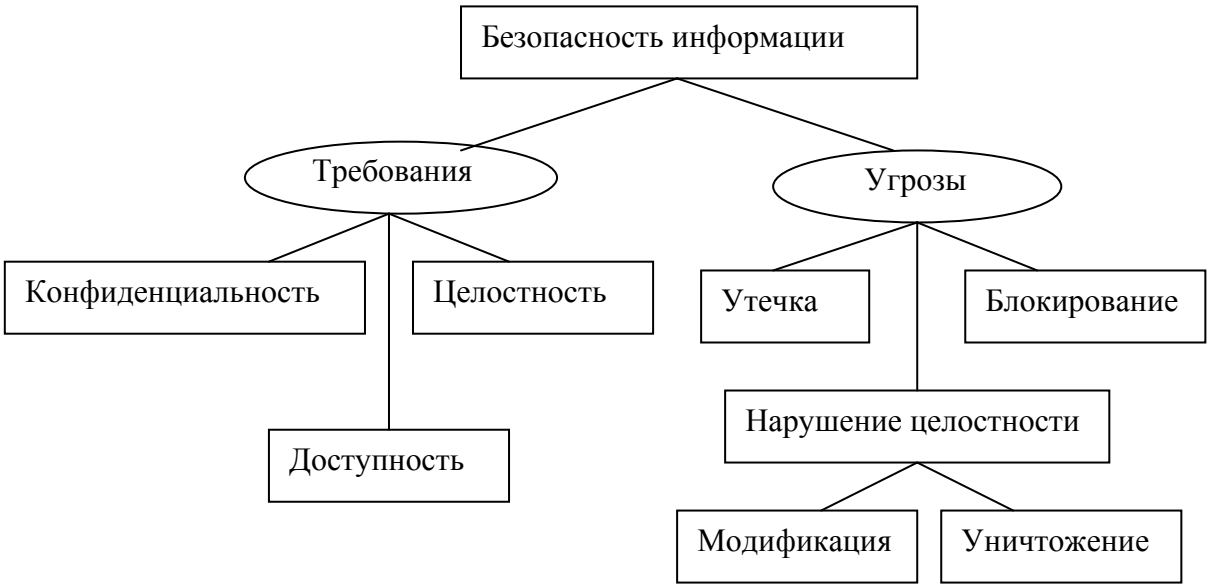

Рис. 3. Требования и угрозы для обеспечения информации.

Часть конфиденциальной коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Коммерческая тайна, в соответствии с гражданским законодательством РФ [1, статья 139], это информация которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель принимает меры к охране ее конфиденциальности. Следовательно, коммерческая тайна не может быть общеизвестной и общедоступной информацией, открытое ее использование несет угрозу экономической безопасности предпринимательской деятельности, потере конкурентных преимуществ, в связи с чем предприниматель осуществляет меры по сохранению ее конфиденциальности и защите от незаконного использования. По функционально-целевому признаку можно выделить следующие составляющие коммерческой тайны [51, с.89-92]:

- Научно-техническая информация (содержание и планы научно-исследовательских работ, содержание “ноу-хау”, рационализаторских предложений, планы внедрения новых технологий и видов продукции).
- Производственная информация (технология, планы выпуска продукции, объем незавершенного производства и запасов, планы инвестиционной деятельности).
- Деловая информация (сведения о контрагентах, конкурентах, потребителях, деловых переговорах, коммерческая переписка, сведения о заключенных и планируемых контрактах).
- Организационно-управленческая информация (сведения о структуре управления фирмой не содержащиеся в уставе, оригинальные методы организации управления, система организации труда).
- Маркетинговая информация (рыночная стратегия, планы рекламной деятельности, планы обеспечения конкурентных преимуществ по сравнению с продукцией других фирм, методы работы на рынках, планы

сбыта продукции, анализ конкурентоспособности выпускаемой продукции).

- Финансовая информация (планирование прибыли, себестоимости, ценообразование – методы расчета, структура цен, скидки, возможные источники финансирования, финансовые прогнозы).
- Информация о персонале фирмы (личные дела сотрудников, планы увеличения (сокращения) персонала, содержание тестов для проверки вновь принимаемых на работу).
- Программное обеспечение (программы; пароли, коды доступа к конфиденциальной информации, расположенной на электронных носителях).

Раскрытие сведений, составляющих коммерческую тайну, способно привести к значительным негативным последствиям для инновационной фирмы, создать серьезные угрозы экономической безопасности как для фирмы в целом, так и для работающего в ней персонала. По оценкам экспертов, потеря лишь четверти информации, относимой к категории коммерческой тайны, обеспечивает весомые преимущества конкурентам и в течение нескольких месяцев приводит к банкротству половины инновационных фирм, допустивших утечку сведений [151]. В связи с этим, есть все основания полагать, что в России по мере развития рыночных отношений с присущими им конкуренцией и хозяйственным расчетом подходы к охране коммерческой тайны радикально изменятся. Для этого необходимо четко представлять информационные угрозы деятельности предпринимательских структур, результатом которых может стать разглашение коммерческой тайны и, как следствие, потеря конкурентного преимущества.

Так, В.И. Ярочкиным приводятся следующие оценки угроз инновационного предпринимательства в российской экономике, сделанные на основе экспертных оценок (табл.2) [118, с.102].

Однако не вся информация, которой располагает предприниматель, может быть отнесена к категории коммерческой тайны. Существует официально утвержденный перечень сведений, которые не могут составлять коммерческую тайну в РФ (Приложение 3) [12].

Соответственно, не вся информация является закрытой для внешних пользователей. Инновационные предприниматели, в плане защиты наиболее важной информации, решают сложную проблему. С одной стороны, они должны предоставить максимум информации о своей деятельности потребителям, контрагентам, кредиторам и т.п. Реклама привлекает покупателей, деловые связи, патенты и лицензии, “ноу-хау” - контрагентов, финансовое положение – инвесторов.

С другой стороны, предприниматели должны оградить названные группы лиц, а также своих конкурентов от информации, утечка или разглашение которой может представлять угрозу их экономической безопасности, лишить предпринимательскую структуру конкурентного преимущества.

Таблица 2

Экспертные оценки угроз инновационного предпринимательства в российской экономике

1. Экономическое подавление		
	- срыв сделок и иных соглашений	48 %
	- парализация деятельности фирм с использованием полномочий государственных органов, средств массовой информации	31%
	- компрометация деятельности фирмы	11%
	- шантаж, компрометация руководителей и отдельных сотрудников	10%
2. Физическое давление		
	- ограбление и разбойное нападение на офисы, склады	73%
	- угрозы физических расправ	22%
	- наемные убийства	5%
3. Промышленный шпионаж		
	- подкуп сотрудников	43%
	- передача документов и разработок	10%
	- копирование программ и данных	24%
	- проникновение в ПЭВМ	18%
	- подслушивание переговоров	5%
4. Финансовое подавление		
5. Психологическое подавление		

В выборе “золотой середины”, то есть определении того оптимального количества информации, которого будет достаточно для внешних пользователей и которое не будет представлять угроз экономической безопасности предпринимательской деятельности и не отразится на конкурентоспособности хозяйствующего субъекта, и состоит первый шаг инновационных предпринимателей в процессе защиты информации, составляющей коммерческую тайну.

Получить информацию о деятельности фирмы можно двумя способами:

- законным (статьи о фирме и финансовые отчеты в открытых источниках, рекламные материалы с выставок и конференций, интервью руководителей фирмы и т.д.);
- незаконным, т.е. получение информации, не предназначенной для внешних пользователей, без согласия руководства фирмы, с нарушением действующего законодательства и приводящее к прямым экономическим потерям от предпринимательской деятельности, потере конкурентоспособности коммерческой фирмы либо к упущенной выгоде.

Существует большое количество способов получения информации об инновационных фирмах и их персонале.

Таблица 3.

Источники получения информации об инновационных фирмах

1.Сбор информации, содержащейся в средствах массовой информации, включая официальные документы, например, судебные отчеты	**11%**
2.Использование сведений, распространяемых служащими конкурирующих фирм	**12%**
3.Биржевые документы и отчеты консультантов; финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм	**12%**
4.Изучение продукции конкурирующих фирм; использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов)	**14%**
5.Замаскированные опросы и «выуживание» информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях, симпозиумах)	**10%**
6.Непосредственное наблюдение, осуществляемое скрытно	**5%**
7.Беседы о найме на работу со служащими конкурирующей фирмы (хотя опрашивающий вовсе не намерен принимать данного человека в свою фирму)	**4%**
8.Так называемые «ложные» переговоры с фирмой-конкурентом относительно приобретения лицензии	**6%**
9.Наем на работу служащего конкурирующей фирмы для получения требуемой информации	**5%**
10.Подкуп служащего конкурирующей фирмы или лица, занимающегося ее снабжением	**3%**
11.Использование агента для получения информации на основе платежной ведомости фирмы-конкурента	**5%**
12.Подслушивание переговоров, ведущихся в фирмах-конкурентах	**6%**
13.Перехват электронных сообщений	**2%**
14.Подслушивание телефонных разговоров	**3%**
15.Кража чертежей, образцов, документации	**1%**
16.Шантаж и вымогательство	**1%**

Так, например, американский журнал «Chemical engineering» опубликовал данные проведенного анкетирования 350 ведущих коммерческих фирм США. По результатам опроса чаще всего назывались 16 источников получения информации (табл. 3).

Анализ причин потери информации в предпринимательской сфере показывает, что в действительности подавляющее большинство случаев связано с ошибками или преднамеренными действиями персонала фирмы.

На рис.4. приведена интересная статистика (по данным Computer Security Institute) [24].

Рис.4. Распределение потерь информации по различным причинам.

Письменный опрос (анкетирование) 250 московских бизнесменов, проведенный летом 2006 года показал, что наиболее типичными формами и методами экономического шпионажа они считают следующие: (табл. 4) [Материал предоставлен сотрудниками отдела СЗИ фирмы ВИТ].

Таблица 4.

Распределение ответов московских бизнесменов о наиболее типичных формах несанкционированного доступа к коммерческим секретам конкурирующих фирм

1.Подкуп или шантаж сотрудников фирмы	**43%**
2.Съем информации с ПЭВМ спецтехникой (проникновение в базы данных, копирование программ)	**42%**
3.Копирование или хищение документов, чертежей, экспериментальных и товарных образцов	**10%**
4.Прослушивание телефонных разговоров, подслушивание разговоров в помещениях и автомобилях	**5%**

Любопытно сравнить результаты этого опроса с мнением группы экспертов стран Общего рынка за тот же год о формах и методах несанкционированного доступа к коммерческим секретам конкурирующих фирм (табл.5) [134]:

Таблица 5.

Распределение ответов группы экспертов стран Общего рынка о наиболее типичных формах несанкционированного доступа к коммерческим секретам конкурирующих фирм

1.Подкуп или шантаж сотрудников фирмы, внедрение туда своих агентов	**42%**
2.Съем информации с ПЭВМ спецтехникой	**35%**
3.Копирование или хищение документов, чертежей, экспериментальных и товарных образцов	**13%**
4.Прослушивание и подслушивание	**5%**
5.Другие способы	**5%**

Как видно из приведенных таблиц, выводы обеих групп заинтересованных лиц поразительно близки друг другу. Что же касается условий, способствующих утечке коммерческих секретов фирм, то опрос 3-х тысяч респондентов в семи городах России, проведенный московским центром по изучению проблем недобросовестной конкуренции в 2006-м году, дал следующие результаты (табл.6) [151]:

Таблица 6.

Распределение ответов группы экспертов в ходе опроса, проведенного московским центром по изучению проблем недобросовестной конкуренции

1.Болтливость сотрудников, особенно в связи с потреблением алкоголя и в дружеских компаниях	**32%**
2.Стремление сотрудников заработать деньги любым способом, по принципу "деньги не пахнут"	**24%**
3.Отсутствие службы безопасности фирмы	**14%**
4."Совковая" привычка сотрудников "делиться передовым (и иным) опытом", давать советы посторонним	**12%**
5.Бесконтрольное использование информационных и копировальных средств на фирме	**10%**
6.Психологические конфликты между сотрудниками, между сотрудниками и руководством, набор случайных людей, жаждущих "продаться" или "отомстить"	**8%**

Получить достоверную информацию о деятельности фирмы незаконным путем маловероятно, если фирма с пониманием относится к сохранности своих ноу-хау и создания соответствующей системы защиты. Кроме того, следует учитывать мировой опыт по защите ноу-хау. В разных странах существуют различные приоритетные направления защиты ноу-хау (промышленных

секретов). Так, в Германии преобладают законодательные меры, в США и Франции, наряду с ними, предпочтение отдается организации собственных служб безопасности фирм, для Японии характерен корпоративный дух и долгосрочная занятость в фирме, в Великобритании защита обеспечивается договорными обязательствами [103]. Идея, что ноу-хау является деловым капиталом, дающим конкурентное преимущество на рынке, представляет собой первооснову организации защиты промышленных секретов в зарубежных фирмах. Поэтому в их практике особое внимание уделяется письменным обязательствам каждого сотрудника о неразглашении промышленных секретов.

В то же время многие российские руководители инновационных структур под безопасностью понимают, прежде всего, физическую защищенность, иногда включая отдельные требования информационной защиты научных, промышленных и коммерческих интересов, что не способствует решению проблем безопасности в комплексе.

На основе вышеизложенных фактов и подводя итог первой главе работы, можно сделать следующие выводы:

- На современном этапе развития инновационного бизнеса информационная защита играет ключевую роль в обеспечении экономической безопасности субъектов предпринимательской деятельности. Это связано со стремительным развитием и внедрением информационных технологий во все бизнес-процессы инновационного предпринимательства и возросшей в связи с этим вероятности угроз деятельности этих объектов.
- Разработка грамотной стратегии обеспечения информационной безопасности является одной из ключевых задач обеспечения конкурентоспособности субъектов инновационного предпринимательства как на национальных, так и на мировых рынках.
- Каждый хозяйствующий субъект должен строить свою систему защиты информации на концептуальной основе, исходя из назначения данного субъекта, его размеров, условий размещения, характера деятельности и т.д.
- При разработке политики защиты необходимо исходить из детального анализа направлений деятельности инновационной фирмы и комплексных требований защиты. Особенно, если структуры применяют в своей деятельности средства информатики.
- Учитывая многообразие потенциальных угроз информации в системе обработки данных, сложность структуры и функций, а также участие человека в технологическом процессе обработки информации, цели защиты информации могут быть достигнуты только путем создания системы защиты информации на основе комплексного подхода.
- Начинать создание системы надо с оценки угроз информационной безопасности деятельности инновационной фирмы, и уже исходя из полученных результатов анализа, принимается решение о построении всей системы защиты и выбираются необходимые средства.

ГЛАВА 2. АНАЛИЗ МЕТОДОВ ФОРМИРОВАНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРОМЫШЛЕННОЙ КОНТРРАЗВЕДКИ НА ПРЕДПРИЯТИЯХ ИННОВАЦИОННОЙ СФЕРЫ

2.1. Методы промышленного шпионажа в России и способы его предотвращения на предприятиях инновационного сектора экономики.

Промышленный шпионаж существовал всегда, по крайней мере, со времен Прометея, который осуществил несанкционированную другими богами передачу людям совершенно секретной технологии получения огня, что впоследствии привело к космическим полетам. Человек всегда стремился знать как можно больше о соседях. В нашу постиндустриальную эру информация приобрела решающую роль.

В большинстве индустриально развитых стран информация является первоосновой всех аспектов развития общества. Преимущество и специфика информации заключается в том, что она не исчезает при потреблении, не передается полностью при обмене (оставаясь в информационной системе и у пользователя), является "неделимой", т. е. имеет смысл только при достаточно полном наборе сведений, что качество ее повышается с добавлением новой информации. Действительно, общество, научно-техническая, производственно-практическая, теоретическая деятельность которого основана на оперативно накапливаемой, разумно используемой информации, в принципе получает в свое распоряжение ресурсы огромной значимости, доступные многократному и многостороннему использованию, дальнейшему "возобновлению" в усовершенствованном виде и быстрому созданию новых информационных систем. Информация - это, во-первых, знание относительно нового типа, пригодное для дальнейшего использования, а, во-вторых, знание, производство, хранение и применение которого действительно становится все более важной для общества деятельностью, порождает соответствующие ему технико-организационные структуры [51]. Одной из таких структур являются организации, занимающиеся несанкционированным получением информации, с целью извлечения прибыли, то есть промышленным шпионажем. Правда, в этой области человечество накопило значительный опыт.

Самыми ранними источниками получения сведений в эпоху, когда человек верил во вмешательство в его дела сверхъестественных сил, были пророки, провидцы, оракулы, прорицатели и астрологи. Если боги заранее знали, что случится в будущем - поскольку они сами до известной степени предопределяли ход событий, - было логично искать указаний о божественных намерениях в откровениях святых людей, в загадках оракулов, в расположении звезд, а часто и в сновидениях.

К 400 году до н.э. Восток значительно опередил Запад в искусстве разведки. Сунь Цзы писал: "То, что называют предвидением, не может быть получено ни от духов, ни от богов...ни посредством расчетов. Оно должно быть добыто от людей, знакомых с положением противника" [42]. С этого начался шпионаж, в том числе промышленный. Очень преуспели в нем многие государи и частные лица. Прекрасно поставленная служба разведки

помогала купцам Венеции и банкирскому дому Фуггеров, фирме Круппа и дому Ротшильдов. Методы практически не менялись столетиями: подкупали, шантажировали, посылали послов-шпионов, перехватывали письма, читали пергаменты (позже книги и газеты) в библиотеках и монастырях. Когда удавалось, подсматривали и подслушивали. Трудности возникали и тогда: надо было передавать полученную информацию в центр сбора и обработки. Для этого приходилось гнать не всегда надежных гонцов, лично пробегать марафонскую дистанцию или пользоваться голубиной почтой. А чтобы не забыть по дороге, о чем шла речь, содержание перехваченных переговоров записывали, а иногда и шифровали. Таким образом, мы видим прообраз технической системы съема информации:

- микрофон, фотоаппарат, камера - ухо или глаза шпиона;
- диктофон или система накопления информации - записки;
- радиоканал, провода и т.д. - гонец;
- приемник - лицо, принявшее сообщение у гонца.

Что касается анализа полученной информации, то все осталось без изменений нужен человек или группа людей, умеющих думать. Единственно, их работу сейчас несколько облегчила вычислительная машина.

Развитие техники вплоть до начала XX века не влияло на средства несанкционированного съема информации: сверлили дырки в стенах и потолках, использовали потайные ходы и полупрозрачные зеркала, устраивались у замочных скважин и под окнами. Появление телеграфа и телефона позволило использовать технические средства получения информации. Гигантское количество сообщений стало перехватываться, влияя на ведение войн и положение на бирже. В 30-40 годы появились диктофоны, действительно миниатюрные фотоаппараты и различные радиомикрофоны. В дальнейшем все большее значение приобретал перехват данных, обрабатываемых в компьютерах, но совершенствовались и традиционные средства. Им, в основном, и посвящена эта небольшая книга.
Что касается России, то до революции у нас существовал достаточно развитый рынок услуг по получению сведений о конкурентах [73], благо отставных "профи" из эффективно работающей охранки было достаточно.
В Советской России коммерческая тайна была отменена официально Положением о рабочем контроле, принятом ВЦИК в ноябре 1917 года. Вместо рынка была введена распределительная система, конкуренцию заменили на соцсоревнование, а всех граждан обязали обмениваться опытом [49]. Государственную и военную тайну охраняли тысячи людей, а эффективности внешней разведки могли на Западе только позавидовать.
Развитие рыночных отношений, развал системы жесткого контроля за производством специальной техники и ввоз ее в страну по официальным и неофициальным каналам, уход из бывшего КГБ, а также ГРУ и МВД профессионалов привел к возрождению промышленного шпионажа в России буквально за два три года. И многочисленным "профи", действующим осторожно и эффективно, прибавились шпионы-любители, начитавшиеся детективов. Сотрудникам "Лаборатории ППШ" приходилось сталкиваться и с

бывшими инженерами-химиками, и с музыкантами, и со студентами, возомнившими себя Джеймсами Бондами. Да и мафиозные группировки в последнее время все больше внимания уделяют получению информации по техническим каналам. Для этого создаются небольшие организации из доверенных людей, на обучение и экипировку которых не скупятся. Многие службы безопасности коммерческих структур успешно проводят операции по внедрению людей и техники конкурентам. Они же очень жестко вынуждены контролировать своих сотрудников с целью недопущения утечки информации о собственных секретах. Нельзя забывать, что интеграция России в международные организации, участие в интернациональных проектах, колоссальный технологический и научный задел в целом ряде направлений делает отечественных предпринимателей объектом пристального внимания частных и государственных служб разведки Запада и Востока.

Как работают государственные структуры, можно показать на примере Военно-промышленной комиссии (ВПК). ВПК имела ряд задач:

1. сбор заявок различных министерств, связанных с военной промышленностью;
2. разработка на основе этих заявок разведывательного плана на год;
3. передача этого плана различным разведорганам (КГБ, ГРУ, службам разведки стран Восточной Европы и т.д.;
4. сбор данных, полученных разведывательными службами за год;
5. подсчет сэкономленных средств в промышленности и научно-исследовательской деятельности.

В контроле выполнения плана помогал ей Всесоюзный институт межотраслевой информации (ВИМИ), своего рода трансмиссия между промышленностью и разведорганами. Высшее руководство осуществлялось Политбюро и ЦК КПСС. Годовой разведплан утверждался лично Генеральным секретарем.

В КГБ задача добывать "специальную информацию" была возложена на управление "Т". Первого главного управления. Это управление занималось, в частности, разведывательной деятельностью в области ядерной промышленности, военного и космического ракетостроения, кибернетики и общей промышленной технологии. Работа проводилась в тесном сотрудничестве с разведслужбами восточноевропейских стран, с которыми постоянные связи поддерживал отдел "Д".

Управление "Т" КГБ отсылало в каждую резидентуру разведплан. На офицеров "линии Х" была возложена задача выполнять все установки плана. Он представлял собой объемный альбом и хранился в посольстве. В свою очередь, ГРУ располагало "оперативным отделом", а именно, "отделом научно-технической разведки", в задачу которого входил сбор научной информации, находившей применение в военной сфере. Каждый год в распоряжение ВПК выделялся специальный фонд около 12 миллиардов франков, для финансирования конкретных операций по сбору информации о западной технике. Эти средства предоставлялись за счет конкретных заказчиков, то есть отраслей производства [55].

Не отстают и США. Впервые в истории там объединена под началом ЦРУ деятельность всей агентуры "разведывательного сообщества". На техническое переоснащение американской разведки до 2010 года выделено порядка 100 миллиардов долларов. Все это не случайно, так как на органы разведки возлагаются задачи по контролю за выполнением экономических соглашений, выявлению незаконной экономической практики и действий, наносящих ущерб интересам США, по оценке запасов сырьевых ресурсов и новой торговой стратегии, возможных прорывов в технологии. Диапазон требований к разведке весьма широк: от анализа общих тенденций до изучения отдельных контрактов [86]. В принципе решен вопрос о передаче добываемой информации частным лицам и организациям.

По аналогии с разведслужбами в деле промышленного шпионажа, только в более скромных масштабах, действуют практически все корпорации, так как это является непременным условием их выживания в условиях жесткой конкурентной борьбы. Обострившаяся на почве научно-технического прогресса конкуренция еще беспощаднее бьет отстающих. Ареной напряженной борьбы стало соперничество за превосходство на рынке, на важнейших направлениях научно-технического прогресса.

Известно, что промышленный шпионаж ведется с целью завоевания рынков сбыта за счет выброса на него новых товаров и продукции повышенного качества и более экономной и совершенной технологии их изготовления, а также путем дискредитации и устранения на нем своих конкурентов любыми методами и средствами. Очевидно, что объектами конфиденциальных интересов со стороны служб промышленного шпионажа выступают производственные структуры, фирмы, корпорации, ассоциации, заводы, предприятия и организации, выпускающие (разрабатывающие) новую продукцию или изделия. Это могут быть отдельные цехи, лаборатории, испытательные площадки, технологические линии, станочный парк, технологическая оснастка и т.п., сведения о которых могут характеризовать состояние производства (включая и систему управления, финансов и т.п.) и выпускаемую продукцию, позволяет оценить качество выпускаемой продукции, уровень издержек производства, его производственные мощности и другие параметры и характеристики, связанные не только с производством и его организационными особенностями и финансовым состоянием.

Результатом конкретной производственной деятельности промышленности является изделие как технический объект [101]. Технический объект - весьма широкое понятие. Им может быть отдельное устройство, любой элемент устройства или комплекс взаимосвязанных устройств. Каждый технический объект имеет определенную функцию, обеспечивающую реализацию соответствующий потребительской потребности. К техническим объектам относятся отдельные машины, аппараты, приборы, сооружения и другие устройства, выполняющие определенные функции по преобразованию, хранению или транспортированию вещества, энергии или информации. К техническим объектам относится любой элемент (агрегат, блок, узел, сборочная единица, деталь и т.п.), входящий в машину, аппарат, прибор и т.д., а также

любой из комплексов функционально взаимосвязанных машин, аппаратов, приборов и т.д. в виде системы машин, технологической линии, цеха и т.п. Из изложенного вытекает, что понятие технического объекта, в случае промышленного шпионажа, выступающего как объект конфиденциальных интересов, весьма многогранно и с позиции системного анализа иерархично. Это может быть большая техническая система, типа акционерного общества, со значительным количеством заводов или отдельное устройство бытового назначения типа электрического фена.

Каждый технический объект предназначается для удовлетворения конкретной потребительской функции. Функция, реализуемая техническим объектом, отражает и описывает его назначение:

- какое действие производит технический объект?
- на какой объект (предмет труда) направлено это действие?
- при каких особых условиях и ограничениях выполняется это действие?

В этом описании и содержится информация о предмете труда - объекте. Злоумышленник имеет дело с информацией, освещающей те или иные стороны объекта его конфиденциальных интересов. Что же будет интересовать злоумышленника? Естественно, информация о производстве и производимой продукции, об организационных особенностях и финансах, о товарном обороте и системе сбыта, о ценах, рекламе, обслуживании и т.п. информация о фирме, предприятии, которая позволит ему найти решение для успешной борьбы со своими конкурентами.

Предпринимательская деятельность тесно взаимосвязана с получением, накоплением, обработкой и использованием разнообразных информационных потоков, поступающих от различных источников. Что следует понимать под источником вообще и под источником конфиденциальной информации, в частности? С некоторой степенью обобщения и с определенным допущением можно привести следующие категории источников, обладающих, владеющих или содержащих в себе конфиденциальную информацию:

1. Люди.
2. Документы.
3. Публикации.
4. Технические носители.
5. Технические средства обеспечения производственной трудовой деятельности.
6. Продукция.
7. Промышленные и производственные отходы.

Коль скоро информация представляет определенную цену, то факт получения информации злоумышленником приносит ему определенный доход, ослабляя тем самым возможности конкурента. Любопытный перечень способов получения информации о своих конкурентах опубликовал американский журнал "Chemical Engineering" [99]:

1. Сбор информации, содержащейся в средствах массовой информации, включая официальные документы, например, судебные отчеты.

2. Использование сведений, распространяемых служащими конкурирующих фирм.
3. Биржевые отчеты и отчеты консультантов, финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм; отчеты коммивояжеров своей фирмы.
4. Изучение продукции конкурирующих фирм; использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов).
5. Замаскированные опросы и "выуживание" информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях, симпозиумах).
6. Непосредственное наблюдение, осуществляемое скрытно.
7. Беседы о найме на работу со служащими конкурирующих фирм (хотя опрашивающий вовсе не намерен принимать данного человека на работу в свою фирму).
8. Так называемые "ложные" переговоры с фирмой-конкурентом относительно приобретения лицензии.
9. Наем на работу служащего конкурирующей фирмы для получения требуемой информации.
10. Подкуп служащего конкурирующей фирмы или лица, занимающегося ее снабжением.
11. Использование агента для получения информации на основе платежной ведомости фирмы-конкурента.
12. Подслушивание переговоров, ведущихся в фирмах-конкурентах.
13. Перехват телеграфных сообщений.
14. Подслушивание телефонных переговоров.
15. Кражи чертежей, образцов, документации и т.п.
16. Шантаж и вымогательство.

С учетом рассмотренного можно определить способ несанкционированного доступа к источникам конфиденциальной информации как СОВОКУПНОСТЬ ПРИЕМОВ, ПОЗВОЛЯЮЩИХ ЗЛОУМЫШЛЕННИКУ ПОЛУЧИТЬ ОХРАНЯЕМЫЕ СВЕДЕНИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА. С учетом этой формулировки приведем систематизированный перечень способов на высоком уровне абстракции. По нашему мнению способами несанкционированного доступа к конфиденциальной информации являются:

1. Инициативное сотрудничество.
2. Склонение к сотрудничеству.
3. Выпытывание, выведывание.
4. Подслушивание переговоров различными путями.
5. Негласное ознакомление со сведениями и документами.
6. Хищение.
7. Копирование.
8. Подделка (модификация).

9. Уничтожение (порча, разрушение).

Согласившись с тем, что перечень источников конфиденциальной информации также независим и не пересекаем на данном уровне абстракции, можно попытаться провести анализ их взаимосвязи и взаимозависимости. Даже беглый обзор позволяет заключить, что к определенным источникам применимы и определенные способы. Как разнообразны источники, так и разнообразны способы несанкционированного доступа к ним. Мы допускаем возможность декомпозиции способов несанкционированного доступа и источников по их применимости в зависимости от определенных условий и ситуаций. Тем не менее, имея формальный набор источников и способов несанкционированного доступа к ним, возможно на допустимом уровне абстракции построить формальную модель взаимосвязи источников и способов на качественном уровне с определенной степенью условности. Такую модель можно было бы назвать обобщенной моделью способов несанкционированного доступа. Теперь рассмотрим существо и возможные реализации способов несанкционированного доступа.

Инициативное сотрудничество.

Известна печальная статистика, говорящая, что 25 процентов служащих предприятия готовы в любое время при любых обстоятельствах предать интересы фирмы, 50 процентов готовы это сделать в зависимости от обстоятельств и лишь 25 процентов, являясь патриотами, никогда не предадут интересы фирмы. Финансовые затруднения, политическое или научное инакомыслие, недовольство продвижением по службе, обиды от начальства и властей, недовольство своим статусом и многое другое толкают обладателей конфиденциальной информации на инициативное сотрудничество с конкурентами и иностранными разведками. Наличие такого человека в подразделении производства и управления позволяет злоумышленнику получать важные сведения о состоянии и деятельности предприятия.

Склонение к сотрудничеству.

Склонение к сотрудничеству - это, как правило, насильственное действие со стороны злоумышленника. Склонение или вербовка может осуществляться путем подкупа, запугивания, шантажа. Подкуп при наличии денег - самый прямой и эффективный способ достижения целей, будь то получение секретной информации, нужного решения или защита интересов "дары приносящих" на алтаре государственной бюрократии. Подкуп - сложный процесс, включающий в себя экономический шпионаж в чистом виде.

Склонение к сотрудничеству реализуется в виде реальных угроз или преследования. Преследование - это оказание психического воздействия, выражающегося в оскорблениях и применении телесных повреждений, расправой, уничтожением вещей, имущества, надругательством над малолетними, престарелыми, беспомощными родственниками или близкими.

Весьма близко к склонению лежит и переманивание знающих специалистов фирмы конкурента на свою фирму, с целью последующего овладения его знаниями. История конкурентной борьбы изобилует примерами такого рода.

Выпытывание.

Выпытывание (выведывание, интервьюирование) - это стремление под видом невинных вопросов получить определенные сведения. Ловко маневрируя словами, выражающими вопросы, пытаются выудить если не всю правду, то хотя бы намек на нее. Джон Де Порам, будучи вице-президентов фирмы "General Motors", говорил: "... у нас принято выуживать информацию у конкурентов". Опыт показывает, что это эффективный и достаточно скрытый метод получения информации, осуществляется через ближайшее окружение предпринимателя (секретарей, помощников, шоферов и т.д.), а также ближайших родственников. Выпытывать информацию можно и ложными трудоустройствами.

Подслушивание.

Подслушивание - способ ведения разведки и промышленного шпионажа, применяемый агентами, наблюдателями, информаторами, специальными постами подслушивания. Подслушивание заманчиво тем, что воспринимается акустическая информация и непосредственно человеческая речь, с ее особенностями, окраской, интонациями, определенной эмоциональной нагрузкой, часто содержащая не менее важные моменты, чем собственно прямое содержание. К этому следует добавить, что подслушиваемые переговоры воспринимаются в реальном масштабе времени и в определенной степени могут позволить своевременно принимать определенные решения. Наиболее активно в настоящее время используются следующие способы подслушивания:

- подслушивание разговоров в помещении или автомашине с помощью предварительно установленных радиозакладок ("жучков");
- подслушивание телефонных переговоров, радиотелефонов и радиостанций;
- дистанционный съем информации с различных технических средств за счет их побочных электромагнитных излучений и наводок (перехват).

Существуют и другие методы подслушивания, например, лазерное облучение оконных стекол в помещении, где ведутся "интересные" разговоры. Иногда использую направленное радиоизлучение, которое заставит "откликнуться и заговорить" деталь в телевизоре, в радиоприемнике, в телефоне или другой технике. Но подобные приемы требуют специфических условий и реализуются только довольно сложной и дорогой специальной техникой.

Подслушивание может осуществляться непосредственным восприятием акустических колебаний подслушивающим лицом при прямом восприятии речевой информации, либо восприятием звуковых колебаний, поступающих через элементы зданий и помещений: стены, полы, потолки, дверные и оконные проемы, вентиляционные каналы, системы отопления, а также посредством весьма разнообразных технических средств. Для этого используются различные микрофоны акустического или контактного восприятия звуковых колебаний, радиомикрофоны, именуемые еще радиозакладками, лазерные средства

подслушивания, специальные методы подслушивания телефонных переговоров и другие методы и средства.

Наблюдение.

Наблюдение - способ ведения разведки о состоянии и деятельности противника. Ведется визуально и с помощью оптических приборов. "Видеть - значит различать врага и друга и окружающее во всех подробностях..." - писал известный физик С.Н. Вавилов.

Наблюдения различаются по виду, длительности, интенсивности и целям. Кроме того, наблюдение может быть разовым, выборочным, периодическим, постоянным, длительным и т.д. Наблюдение может вестись за неподвижными (стационарными) объектами со стационарных позиций или подвижным наблюдением и за подвижными объектами: люди, технические средства (автомашины, поезда, самолеты, корабли и т.п. средства передвижения). Наблюдение может вестись на расстоянии прямой видимости и на больших расстояниях с помощью специальных оптических систем и систем телевидения.

К техническим средствам наблюдения относятся:

- бинокли, подзорные и стереотрубы и другие системы визуального наблюдения при обычном освещении в пределах определенной видимости;
- телевизионные системы дальнего наблюдения; - инфракрасные системы и приборы ночного видения для условий ограниченной видимости или для ночных условий.

Для наблюдения эти технические средства могут быть использованы как в бытовом исполнении, приобретаемые в обычных магазинах (они меньше привлекают своей обычностью), так и специального криминального исполнения (бинокль со встроенным фотоаппаратом, скрытые телевизионные камеры и др.) Используются системы скрытного визуального наблюдения из автомобиля. Например, система РК-1780 позволяет вести наблюдение с использованием оптики, вмонтированной в автомобильную антенну. Объектив имеет диаметр 5 мм. Объектив соединен с салоном посредством волоконно-оптического кабеля, объектив может поворачиваться по азимуту, имеет угол обзора 70о, фокусное расстояние - от 3 м до бесконечности. К волоконно-оптической системе можно подключить (присоединить) фото- или кинокамеру.

Используют специальные системы и для наблюдения за помещениями без непосредственного проникновения в них. Так, система наблюдения типа РК-1715, имеющая волоконно-оптический кабель длиной от 0,9 до 1,8 метра позволяет вести наблюдения в особо сложных условиях через вентиляционные шахты, фальшь - потолки, кабельные и отопительные вводы и т.п. проходные системы. Угол обзора системы 65о; фокусировка - от 10 мм до бесконечности. Работает при слабом освещении. Возможно сопряжение с фотоаппаратурой. При фокусном расстоянии 10 мм можно читать и фотографировать текст документов, записи в календаре и другие материалы. Особое место в наблюдении отводится телевидению.

Технические средства позволяют вести наблюдения за подвижными средствами. Для слежки за маршрутом движения автомобилей в них монтируются радиомаяки, позволяющие бригадам наружного наблюдения определять приближение к ним или удаление от них наблюдаемого средства или с помощью пеленгаторных устройств определять местонахождение с определенной степенью точности. Такие радиомаяки включаются в работы при включении зажигания автомобиля, чем сообщают о начале движения наблюдаемого средства.

Наблюдение, как способ добывания информации, относится к эффективным средствам добывания и, по-прежнему широко используется, хотя бы уже потому, что оснащается новейшими техническими средствами.

Хищение.

Хищение - умышленное противоправное завладение чужим имуществом, средствами, документами, материалами, информацией. Этим незаконным способом в условиях рыночной экономики широко пользуются злоумышленники как для получения коммерческих секретов, связанных с производством и реализацией товаров народного потребления. Естественно, завладение информацией путем хищения проводится скрытно (тайно) от окружающих.

Зачастую хищение обусловливается определенными, удобными для этого условиями. В [112] указывается, что:

- 10 % людей никогда не воруют, ибо это не совместимо с их моралью;
- 10 % людей воруют при каждом удобном случае, при любых обстоятельствах;
- 80 % людей, как правило, честные, за исключением тех случаев, когда предоставляется случай украсть.

Воруют документы, воруют продукцию, воруют переносные магнитные накопители, воруют ключи и коды секретных сейфов и хранилищ, воруют пароли и шифры и т.д. и т.п.

Копирование.

В практике криминальных действий копируют документы, содержащие интересующую злоумышленника информацию; копируют технические носители; копируют информацию, обрабатываемую в АСОД; копирую производимую продукцию.

Подделка (модификация, фальсификация).

В условиях конкуренции подделка, модификация, имитация приобретают все большие масштабы. Подделывают доверительные документы, позволяющие получить определенную информацию; подделывают письма, счета, бухгалтерскую и финансовую документацию; подделывают ключи, пропуска, пароли, шифры, продукцию и т.п. Известно, что даже незначительная модификация программ в АСОД может обеспечить злоумышленнику возможность несанкционированного получения конфиденциальной информации. По подложным документам возможно получение не только денежных сумм, но и продукции, элементов, материалов, представляющих для злоумышленника коммерческий интерес.

Подделка продукции может принести огромный материальный ущерб. Подделка так порой имитирует настоящую продукцию, что нередко даже самим специалистам трудно установить, где фальшивка, а где подлинник. Дело в том, что подпольные фирмы налаживают производство подделок по той же технологии, с использованием тех же узлов, что и компания с мировым именем. Начало подпольному производству дают шпионы, которые крадут не только секреты, но по подложным документам получают важнейшие узлы и компоненты изделий.

Подделка используется для выдачи себя за другого пользователя, чтобы снять с себя ответственность или же использовать его полномочия с целью формирования ложной информации (дезинформации), применения ложного удостоверения личности для получения санкционированного доступа к охраняемым сведениям, не только при непосредственном общении, но и при общении в системах связи и АСОД. В АСОД к проблеме подделки кроме того относят, в частности, такие злонамеренные действия, как фальсификация - абонент-получатель подделывает полученное сообщение, выдавая его за действительное в своих интересах; маскировка - абонент-отправитель маскируется под другого абонента с целью получения им охраняемых сведений. Не меньшую опасность в вопросах подделки представляют компьютерные вирусы, способные со злоумышленной целью модифицировать программы, наносящие определенный ущерб предприятию в его коммерческой деятельности.

Уничтожение.

В части информации особую опасность представляет ее уничтожение в АСОД, в которых накапливаются на технических носителях огромные объемы сведений различного характера, многие из которых очень трудно изготовить в виде немашинных аналогов. В АСОД, к тому же, находится в интегрированных базах данных информация разнообразного назначения и различной принадлежности.

В преступных руках оказываются эффективные средства уничтожения источников информации и даже объектов конфиденциальных интересов. Пластиковые бомбы, портативные ручные гранаты, различные взрывные устройства прямого действия и дистанционно-управляемые, позволяющие осуществить преступные замыслы. Уничтожаются и люди, и документы, и средства обработки, и продукция. Использование средств уничтожения может быть как тайным (минирование со срабатыванием по времени или по сигналу управления), так и открытым.

Уничтожению подвергаются системы охраны, связи, автоматизированной обработки, защиты информации и т.д. Широкое распространение получили преступления, связанные с порчей или изменением технологии процессов производства, автоматизированной обработки. Уничтожение может совершаться путем поджогов, имитирующих возникновение пожара. Возможен при этом вывод из стоя систем противопожарной защиты и сигнализации.

Значительное место среди преступлений против АСОД занимают саботаж, взрывы, разрушения, вывод из строя соединительных кабелей, систем кондиционирования.

В мире реального бизнеса слову "конкурировать" больше соответствует понятие "уничтожить конкурента любой ценой". Конкуренция - это жестокая борьба. Она ставит конкурентов в такие жесткие условия, что они вынуждены поступать по принципу "победителей не судят, цель оправдывает средства". Вопрос ставится однозначно: или ты, или тебя пустят по миру. Недобросовестная конкуренция осуществляется в форме промышленного шпионажа, коррупции, организованной преступности, фальсификации и подделки продукции конкурентов, манипулирования с деловой отчетностью (подделки, приписки, искажения, подмена и т.д.) и, наконец, путем прямого обмана, грабежа, нанесения материального ущерба. Очевидно, что все виды "оружия" и способы криминальных действий недобросовестной конкуренции используются в зависимости от объектов злонамеренных действий и возможности доступа к объектам и информации.

Получить сколько-нибудь достоверную информацию об объектах конфиденциальных интересов законным путем практически невозможно, поскольку в мире капитала поддерживается определенная система защиты ценной информации от несанкционированного доступа со стороны злоумышленников. Слово "несанкционированного" акцентирует на то, что действия совершаются противоправным путем, в обход этических норм и систем защиты с целью получить конфиденциальную информацию для использования в корыстных целях.

Злоумышленник в своих противоправных действиях всегда выступает субъектом, действия которого направлены на то, что противостоит ему или является объектом его интересов. Известно, что объект - философская категория, выражающая то, что противостоит субъекту в его предметно-практической и познавательной (читай: разведывательной, шпионской) деятельности [62]. В практике военного шпионажа понятие "объект разведки" сложилось давно и не требует каких-либо разъяснений. Так, "объектом работы Р. Зорге в Японии была Япония, а объект - Германское посольство - это только прикрытие". Однозначна трактовка объекта разведки, например, в радиоразведке, в радиолокации и других видах разведки. Объектами наблюдения, например, в радиолокации, являются физические тела, сведения о которых представляют практический интерес [37]. В [94] прямо указывается, что "разведка радиосигналов, излучаемых разведываемыми объектами и разведка изображений самих объектов осуществляется средствами радиоэлектронной разведки", а в [65] ..." секрет создания отравляющих газов не мог не стать объектом промышленного шпионажа. Французскому тайному агенту ... удалось овладеть осколком снаряда при испытаниях ... и вскоре страны Антанты приступили к производству отравляющих газов". Этот самый осколок был источником сведений о составе химического вещества. Любая информация, совмещающая эти направления, представляет большой интерес в плане изучения возможных направлений коммерческой деятельности.

В одном параграфе невозможно даже кратко рассказать о всех возможных методах получения информации. О некоторых авторы умышленно не стали упоминать, потому что еще не пришло время и не хотелось бы создавать трудности в работе государственных органов по защите граждан, т. е. всех нас, от преступников и иностранных шпионов. Кроме того, не хотелось бы, чтобы монография стала своего рода учебным пособием для начинающих шпионов, хотя полностью избежать этого, видимо, не удалось. Для них повторяем, что работа по съему информации не романтическое, а очень опасное дело, требующее специальных навыков, групп прикрытия, "легенд", агентов, больших денег и большого ума.

Надеемся, что бизнесмены, политики, да и просто люди, по разным причинам ставшие носителями коммерческих и других секретов, получили представление о реальных возможностях злоумышленников в России. В дальнейшем, вероятно, выйдет более развернутая работа о спецсредствах и о мерах противодействия им.

2.2. Особенности нормативно-правового регулирования и защиты прав в сфере интеллектуальной собственности в России и зарубежом

24 ноября 2006 года Государственной Думой РФ принят и 18 декабря 2006 года подписан Президентом Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ», содержащей основные нормы в области интеллектуальной собственности.

Указанный закон вводится в действие с 01.01.2008 и с его принятием утрачивают силу ранее принятые нормативные акты в этой области, перечень которых приведен в законе. При этом согласно ст.4 Закона до приведения правовых актов в соответствие с ч.4 Кодекса действующие законы применяются постольку, поскольку они не противоречат ч.4 кодекса. Нормативная база в области интеллектуальной собственности до принятия ч.4 Кодекса состояла в основном из принятых в 1992г. законов «Об авторском праве и смежных правах», «Патентного закона РФ», «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров», «О правовой охране программ для ЭВМ и баз данных», «О правовой охране топологий интегральных микросхем».

На основе этого пакета законов, а также принятых в их развитие ведомственных актов в течение 15 лет в России осуществляется правовое регулирование вопросов охраны и защиты объектов интеллектуальной собственности.

Интеллектуальную собственность (ИС) условно делят на литературно-художественную (авторские и смежные права, программы для ЭВМ, базы данных) и промышленную собственность (патенты, товарные знаки и фирменные наименования, ноу-хау). К промышленной собственности также относят коммерческую тайну, рационализаторские предложения, открытия, селекционные достижения.

В то же время, программы для ЭВМ, охраняемые авторским правом, в ряде случаев могут быть запатентованы, если, например, заявляется

программно-аппаратный комплекс и программа является частью технического решения, в частности, по управлению исполнительным элементом механизма. Понятие интеллектуальной собственности не раскрыто подробно в упомянутых нормативных документах, как и в ст.44 Конституции РФ, ст.128 и 138 ГК РФ, действующих до принятия ч.4 нового Кодекса, но на практике определяется как «совокупность исключительных прав личного и имущественного характера на результаты интеллектуальной деятельности». Этим подчеркивается двойственный характер интеллектуальных прав, что отражено также в ст.1226 нового Кодекса.

Если патентные права в России удостоверяются государством после экспертизы, проведенной Роспатентом, то в области авторских прав нет соответствующего государственного органа. Это обусловлено, в частности, самим характером этих прав, возникающих в силу самого факта создания произведения и обнародования его в любой объективной форме (письменной, устной, магнитной записи и т.д.) и тем, что для осуществления этих прав не требуется специальная регистрация. Тем не менее, зачастую российские авторы регистрируют (депонируют) свои произведения в каком-либо из коллективных обществ по управлению авторскими правами, наиболее часто в РАО (Российском авторском обществе).

Патентные же права требуют обязательной регистрации и без нее недействительны. Однако, во-первых, не все объекты могут патентоваться. Так, не патентуются открытия, научные теории, правила игр, сорта растений и породы животных, решения, противоречащие общественным интересам (например, бесполезные изобретения, наиболее выдающимся из которых присваивается т.н. «Игнобелевская премия» www.patent-bureau.ru/News/ от 28.06.06). Во-вторых, процедура патентования длительная (1-3 года и больше) и затратная. В-третьих, срок действия патента ограничен 20 годами (для некоторых объектов 25 лет), после чего объект становится общественным достоянием.

Поэтому зачастую целесообразнее сохранить технологию, рецепт или особенности конструкции в тайне, как это сделали, например, создатели рецепта «Кока-кола», что дает возможность неограниченного (по времени) владения исключительными правами на охраняемый в тайне объект.

При этом выбор между патентованием или сохранением особенностей разработки в тайне должен быть сделан автором (владельцем) осознанно с учетом поставленных целей, возможности сохранения в тайне и т.д.[1]

Характерной чертой действующего российского законодательства об ИС является его рыночная направленность. Имущественные права на объекты ИС становятся своеобразным товаром, который может свободно отчуждаться и передаваться в результате совершения гражданско-правовых сделок. Обычно утверждается, что свободный рыночный оборот имущественных прав на

---

[1] Выгодин Б.А**.** Защита интеллектуальной собственности в России. Правовые основы, регламентирующие документы. "The Angel investor". 2007.

объекты ИС "поощряет стремление создавать значительные работы и облегчает возможность использования этих работ в коммерческих целях" [2, с. 5].

В то же время нельзя не отметить, что использование в качестве теоретической основы при создании современной законодательной базы концепции исключительных прав привело к значительному отклонению реальных последствий, имеющих место на практике, от тех целей, которым призвано служить право ИС.

Весьма вероятно, что именно чрезвычайное и одностороннее увлечение концепцией исключительных прав при формировании законодательства – одна из причин того, что использование прав ИС приобретает иногда спекулятивный характер, совершенно не соответствующий их назначению. В результате в ряде случаев закрепляемые законодательством права не столько способствуют использованию объектов ИС, сколько блокируют широкое распространение творческих достижений.

Разумеется, в определенной мере это обусловлено отсутствием достаточно развитой законодательной регламентации отношений и практики их договорного оформления в современных условиях. С неудобствами, связанными с негибкостью существующего законодательства в "территориальном" вопросе, сталкиваются многие правообладатели, в частности производители лекарств, пытающиеся поддерживать объективно обусловленную разную ценовую политику в отношении продаваемых препоратов для столичного и региональных рынков.

Однако более негативные последствия имеет то обстоятельство, что низкий уровень законодательной регламентации вопросов, связанных с передачей исключительных прав, на практике поощряет стремление осуществлять "полный выкуп" таких прав без приложения реальных усилий для их дальнейшего использования. Именно с этим обстоятельством связан встречающийся спекулятивный уклон в развитии современного рынка ИС, на котором зачастую права приобретаются не для целей использования, а для их последующей перепродажи. В результате такого подхода некоторые объекты ИС либо совсем не используются, либо используются далеко не всеми возможными способами и в ограниченном масштабе.

Интересно проанализировать, почему в российском законодательстве стало использоваться понятие исключительных прав, каковы были цели его внедрения.

Как известно, в России в течение XIX-XX веков неоднократно менялись законодательно закрепляемые концепции авторских прав. Например, законодательство XIX века (в частности, ст. 420 Свода законов 1887 г.) закрепляло понимание авторского права как разновидности права собственности, отдавая предпочтение охране интересов издателей. В конце XIX века в разработанном законопроекте авторское право предлагалось рассматривать как право относительное, возникающее из договорных отношений. Авторские права понимались то как привилегия, то как особый вид имущества, то как права личности, то как права собственности [83].

Когда Г.Ф. Шершеневич и иные российские юристы в конце XIX - начале XX века настаивали на построении российского законодательства об авторском праве на основе концепции исключительных прав, они, несомненно, видели в такой концепции определенного рода панацею от ранее использовавшихся подходов, которые позволяли заключать кабальные договоры в отношении будущих произведений автора, т. е. планировалось добиться более высокого уровня защищенности интересов творческих работников, а вовсе не предоставить издателям ничем не ограниченное право запрещать использование произведения.

Именно в связи с этим при принятии Закона об авторском праве 1911 г. наряду с закреплением исключительных прав был предусмотрен обширный массив законодательных положений, направленных на пресечение возможных случаев злоупотребления такими правами со стороны правопреемников автора.

В теории гражданского права обычно считается, что в договорных обязательствах правам одной стороны всегда корреспондируют обязанности другой. В то же время на практике в зависимости от вида договора данное обстоятельство оказывается далеко не столь очевидным. Характерно, что в Законе об авторском праве 1911 г. наряду с правами четко определялись именно обязанности сторон, причем особое внимание уделялось правовой регламентации обязанностей пользователя (издателя), наличие которых должно было гарантировать достижение целей заключаемого договора и предоставлять автору возможности для эффективного воздействия на издателя, если его деятельность не обеспечивала достижение таких целей – тиражирование и распространение литературного произведения. Причем все обязанности должны были выполняться в сроки, установленные законом или договором либо соответствующие добросовестной практике.

В советское время широкое распространение получили типовые договоры, которые представляли собой подзаконные акты, характеризовавшиеся нормативностью, обязательностью применения, а также в определенной мере недействительностью отступлений от содержащихся в них условий [105].

Разумеется, обязательность типовых договоров в советский период в ряде случаев приводила к существенному ограничению возможностей сторон свободно определять свои договорные отношения, однако такие договоры способствовали защите интересов авторов благодаря закрепленному в законодательстве правилу о том, что в случаях, когда условия заключенного с автором договора ухудшали его положение по сравнению с положением, предусмотренным в законе или типовом договоре, такие условия признавались недействительными и заменялись условиями, установленными законом или типовым договором.

Отсутствие типовых договоров в настоящее время приводит к значительным негативным последствия. В развитых зарубежных странах договорная практика развивалась и основные формулировки договоров оттачивались на протяжении столетий. К сожалению, в Российской Федерации на сегодня вообще отсутствуют какие-либо общепринятые, апробированные

многолетней практикой применения формы передачи авторских прав, прав на использование изобретений и т. д. Договоры пишутся в зависимости от конкретного случая, часто отличаются низким юридико-техническим уровнем (достаточно упомянуть нередко встречающиеся на практике случаи передачи авторских прав по договору купли-продажи или даже по договору поставки, указания на "продажу всех прав" без конкретизации передаваемых прав, видов использования произведения, территории, сроков и других условий авторского договора), иногда вместо авторского договора заключается трудовой и наоборот. Часто договорное оформление отношений вообще не осуществляется.

Нередко договоры составляются без участия специалистов в области ИС, причем даже юристы организаций при написании договоров иногда ориентируются не на положения действующего законодательства, а на устаревшие подзаконные нормативные акты.

Неправильное оформление передачи прав на практике приводит к нестабильности всего рынка ИС, а также к доминированию в ряде случаев "сильной" стороны (крупных пользователей) над "слабой" (авторами, их наследниками и иными правообладателями).

Государство, как правило, воздерживается от выработки нормативно определенных рекомендаций в данной области, даже несмотря на то, что многие договоры в сфере ИС подлежат государственной регистрации.

Отсутствие нормативных актов, содержащих детальную регламентацию, можно было бы восполнить разработкой рекомендательных норм – типовых договоров, субсидиарно применяемых в случае согласия сторон (ссылки в авторском договоре на соответствующий типовой договор), при отсутствии в договоре условий по тому или иному вопросу (в том числе в качестве формализованного "обычая делового оборота") либо в случае недобросовестного поведения одной из сторон, в том числе включения ею в договор положений, превращающих его в кабальную сделку или рассчитанных на введение другой стороны в заблуждение.

Разумеется, такие типовые договоры не могут и не должны быть обязательными для применения сторонами, однако они значительно способствовали бы развитию деловой, административной и судебной практики, в частности, борьбе со злоупотреблением предоставляемыми правами.

На наш взгляд, при судебном рассмотрении дел, связанных со спорами об условиях договоров в сфере ИС и добросовестности их соблюдения участниками гражданских правоотношений, особое внимание должно уделяться цели, для которой они заключались. Так, цель издательского договора – не приобретение и переуступка прав, а размножение и распространение произведения и т. д. Именно исходя из соответствия таким целям условий договора и действий, предпринятых для его исполнения, и должна устанавливаться "добросовестность" стороны.

Например, как недобросовестное поведение, дающее основание суду для пересмотра условий договора, можно рассматривать неуказание в тексте договора сведений о предполагаемой розничной или оптовой цене издания

либо указание в тексте договора или в предоставляемой правообладателю отчетности явно заниженных цен по сравнению с реально существующими.

Немотивированное отклонение от условий типового договора, существенным образом ухудшающее положение автора, должно рассматриваться как основание для изменения или расторжения договора по требованию введенной в заблуждение стороны.

Как уже отмечалось, в условиях рыночной экономики имущественные права на объекты ИС можно рассматривать как особого рода товар. При этом и правообладатели, и добросовестные пользователи стремятся не к "условной" свободе, обеспечиваемой неточностью и наличием пробелов в правовых формулировках, а к четким правовым моделям взаимодействия друг с другом и с органами государства.

Сложным является вопрос определения базовых положений для регламентации договоров в области ИС. Как известно, в сфере промышленной собственности признается, что обладатель имущественных прав на объект ИС может передать свои права другому лицу по договору об уступке прав или предоставить ему разрешение на использование данного объекта по лицензионному договору (исключительной или неисключительной лицензии). В то же время многие специалисты в области авторского права полагают, что в целях защиты интересов создателей интеллектуальных ценностей недопустимо закреплять в законодательстве возможность полной уступки авторских прав. Действительно, современное российское законодательство закрепляет только возможность предоставления отдельных авторских прав или определенного их перечня по договорам о предоставлении таких прав на исключительной или неисключительной основе. При этом установлены многочисленные презумпции, по существу предписывающие толковать все возможные неясности в договоре в пользу автора или иного правообладателя.

Следует отметить, что многие теоретические положения и законодательные формулировки, полученные в ходе работы над разделом ГК РФ, посвященным вопросам ИС, можно было бы в полной мере использовать при дальнейшей разработке специального законодательства.

Так, на наш взгляд, желательно использовать следующее разграничение понятий "уступки" и "лицензии", предложенное профессором А.П. Сергеевым. По договору об уступке прав на объект ИС обладатель имущественных прав передает или обязуется передать принадлежащие ему права другому лицу, а сам лишается прав, переданных по такому договору. По лицензионному договору о предоставлении разрешения на использование объекта ИС обладатель таких прав (лицензиар) предоставляет или обязуется предоставить другому лицу (лицензиату) разрешение на использование данного объекта в пределах и способами, предусмотренными договором (лицензией). Разумеется, лицензионный договор может предусматривать предоставление лицензиату разрешения на исключительной основе (исключительная лицензия) или на неисключительной основе (неисключительная лицензия), однако в любом случае заключение лицензионного договора не лишает лицензиара прав на соответствующий объект ИС.

Вопрос о том, насколько в авторско-правовой сфере имеет смысл ограничить возможность заключения договоров уступки, нуждается в отдельном рассмотрении.

В ходе работы над разделом ГК РФ, посвященным вопросам ИС, в результате анализа действующих отечественных, зарубежных и международных правовых актов оказалось возможным выделить, в частности, следующие важные положения, касающиеся договоров в области ИС:

1) условия договора об уступке прав или лицензионного договора, ухудшающие положение обладателя прав ИС по сравнению с условиями, предусмотренными законом, являются недействительными; вместо таких условий должны применяться законодательные положения;

2) условия договора об уступке прав или лицензионного договора, ограничивающие право гражданина создавать результаты творческой деятельности, ничтожны;

3) договор, предусматривающий возможность использования объекта ИС, в котором прямо не указывается, что он является договором об уступке прав, должен признаваться лицензионным договором, поскольку именно такой подход в наибольшей степени отвечает интересам правообладателей и достижению определенности в возникающих правоотношениях;

4) права, прямо не указанные в лицензионном договоре, считаются не предоставленными;

5) если иное прямо не предусмотрено лицензионным договором, права считаются предоставленными на неисключительной основе (неисключительная лицензия);

6) права, полученные по лицензионному договору, могут передаваться полностью или частично другим лицам только в случаях, прямо предусмотренных таким договором;

7) если в лицензионном договоре не предусмотрено иное, то лицензиар обязан использовать объект ИС указанными в таком договоре способами;

8) переход имущественных прав ИС к другому лицу не является основанием для изменения или расторжения лицензионного договора о предоставлении разрешения на использование соответствующего объекта ИС;

9) законом может быть предусмотрено, что в отношении отдельных объектов ИС или отдельных прав на них не допускается заключение договоров об уступке прав или лицензионных договоров.

Характерно, что некоторые общепризнанные положения, относящиеся, например, к договорам в области авторского права, не удается включить в перечень основных презумпций, установленных для всех видов объектов ИС в целом. Так, в соответствии с абзацем 2 п. 2 ст. 31 Закона РФ "Об авторском праве и смежных правах" предметом авторского договора не могут быть права на использование произведения, неизвестные на момент заключения договора (так называемые "будущие права"). Очевидно, однако, что такого рода положения не могут быть установлены в отношении объектов патентного права при заключении договоров уступки и тем более в отношении товарных знаков и иных средств индивидуализации.

Несомненно, следует учитывать специфику как отдельных видов объектов ИС, так и отдельных правовых форм, опосредующих использование таких объектов в экономическом обороте, к числу которых обычно относят не только договор об уступке прав и лицензионный договор, но и договоры коммерческой концессии, доверительного управления имущественными правами на объекты ИС, договоры в сфере управления имущественными авторскими и смежными правами на коллективной основе, залог прав на объекты ИС и т. д.

Следует признать, что ввиду большого многообразия объектов ИС и связанных с ними отношений невозможно ограничить правовую регламентацию договорного оформления отношений в данной области только несколькими видами договоров, а тем более включить исчерпывающий перечень допустимых договоров в области ИС в ГК РФ. Гражданское законодательство всегда предусматривало возможность заключения как предусмотренных, так и не предусмотренных Кодексом договоров, а также договоров смешанного типа.

В настоящее время, на наш взгляд, наиболее целесообразны дальнейшая разработка общих положений договорного права в рамках специального законодательства об отдельных видах объектов ИС, подготовка типовых договоров для наиболее массовых и типичных случаев использования таких объектов, доктринальное обобщение результатов, достигаемых в ходе развития правотворческой и правоприменительной практики.

Не вызывает сомнений, что отношения, связанные с использованием результатов интеллектуальной деятельности и средств индивидуализации, будут продолжать развиваться. В результате ждет своего решения вопрос о направлении грядущей эволюции права ИС. Однако попытки научного осмысления понятия ИС, правового регулирования связанных с ней отношений, правового режима результатов интеллектуальной деятельности и средств индивидуализации, отраслевой принадлежности права ИС и других связанных с ИС вопросов породили серьезные разногласия среди ученых-юристов, особенно среди специалистов в области гражданского права.

На наш взгляд, при поиске решений для возникающих противоречий необходимо в каждом случае исходить из главных целей права ИС, чтобы на их основе анализировать различные теоретические подходы, законодательство, судебную и административную практику, практику построения договорных отношений, действующие механизмы реализации и защиты прав, а также направления эволюции права ИС, определять, насколько законодательство об ИС и предлагаемые варианты его развития отвечают целям правового регулирования и какие могут быть предложены меры для обеспечения наибольшего соответствия между целями охраны интеллектуальных ценностей и реально достигаемыми результатами.

Ответы на эти вопросы позволят использовать системный подход при поиске решений для всего комплекса проблем, связанных с охраной и защитой результатов интеллектуальной деятельности, стимулированием развития российского рынка ИС.

Следует принимать решения исходя из требований практики, с учетом необходимости поддержания баланса интересов всех сторон, используя при этом весь накопленный международный и отечественный опыт, а не основываясь исключительно на попытках подчинить новые экономические реалии положениям, выведенным путем схоластического толкования уже закрепленных в законодательстве формулировок, либо полагаясь исключительно на формирование устойчивой судебной практики, хотя во многих случаях необходимый для этого законодательный фундамент отсутствует.

Во Всемирной декларации по интеллектуальной собственности, принятой ВОИС в 1998 г., подчеркивается, что ценность ИС определяется тем, что права ИС:

- стимулируют творческую активность и обеспечивают доступ к результатам творческой деятельности;
- обеспечивают универсальную охрану интересов авторов, пользователей и общества;
- являются одним из самых необходимых условий развития;
- становятся необходимыми элементами привлечения капиталовложений в важнейшие секторы национальной экономики.

Именно ИС является основой культуры и важнейшим условием решения задачи, стоящей перед человечеством на протяжении всей его истории: постоянного роста результатов при постоянном сокращении затрачиваемых на их достижение усилий.

За последние десятилетия роль интеллектуальной собственности в мировой экономике выросла значительно. Перед началом Уругвайского раунда (1986), только компании США теряли около 50 млрд. $[2] в год из-за недостаточного уровня защиты интеллектуальной собственности. Но не только США заинтересованы в чётком правовом регулировании этого вопроса на международном уровне. Вступление России в ВТО, возможно, осуществится уже в ближайшие годы. Россия – государство с богатейшими интеллектуальными ресурсами. Наследие советской науки, современные технические разработки в различных областях, это капитал, который должен быть защищён и работать на благо страны. При устранении таможенных и других барьеров, в результате подписания пакета ВТО, интеллектуальная собственность и товары, связанные с уникальными «ноу-хау», разработки советских и российских учёных и конструкторов могут стать конкурентоспособным товаром.

На сегодняшний день вопросами интеллектуальной собственности в международно-правовом аспекте в основном занимаются две международные межправительственные организации: ВОИС и ВТО, в рамках соглашения по ТРИПС. Как известно ВОИС создана в XIX веке, а с 1974 г., после принятия поправок и дополнений к соглашениям, стала специализированным учреждением ООН.

---

[2] Россия и международная торговля М.

Существуют и другие программы международного сотрудничества в области ИС, в частности, программы в рамках ЮНЕСКО, но нам хотелось бы остановиться на вопросах связанных с ТРИПС и взаимоотношениях ВТО и ВОИС. А так же попытаться ответить на вопрос, почему при наличии такой серьёзной организации как ВОИС возникла потребность в принятии нового соглашения.

В ходе рассмотрения данного Соглашения неизбежно напрашивается сравнение с теми документами, что были выработаны по этому вопросу до Уругвайского раунда.

Соглашение ТРИПС[3] содержит Преамбулу и VII частей.

I - Общие положения и основные принципы. (ст.1 – 8).

Здесь выделяются три основных момента.

Во-первых, утверждается «национальный режим» и «режим наиболее благоприятствуемой нации» в отношении вопросов защиты интеллектуальной собственности. Это статьи 1 п.3, 3 и 4.[4]

Второй, и наиболее интересный момент, это наличие отсылок к Парижскому, Бернскому, Римскому и Вашингтонскому соглашениям (последнее, касающееся вопросов, связанных с защитой топологий интегральных микросхем, формально так и не вступило в силу) по вопросам предоставления национального режима. В частности, в ст.5[5] говорится, что участники соглашений под эгидой ВОИС[6] руководствуются принципами предоставления национального режима, предусмотренными в этих соглашениях. В частности, ст. 2 Парижской Конвенции[7] предусматривает национальный режим относительно патентов.

Подобные отсылки встречаются не только в части I, но и в других, регулирующих конкретные объекты. Здесь некоторые учёные задаются вопросом, как действовать в случае, если в рамках ВОИС будут приняты поправки к соглашениям, не совместимые с принципами Соглашения по ТРИПС. Например, значительно увеличив регулирующую роль государства в таких вопросах, как обязательное лицензирование, что принципиально и идеологически отвергается ВТО.

Цели и принципы Соглашения, как и всего пакета ВТО, можно кратко охарактеризовать как устранение препятствий в осуществлении международной торговли. Здесь под таким препятствием подразумеваются нарушения интеллектуальной собственности, имеющие последствия в экономической сфере.

Часть II (с 9 по 40 статью) Соглашения содержит нормы и стандарты, касающиеся регулирования вопросов, связанных с конкретными объектами интеллектуальной собственности. Соглашение по ТРИПС, а в английской аббревиатуре присутствует «Trade Related», что корректнее переводится не как

---

[3] Документы ВТО скопированы с официального сайта ВТО www.wto.org
[4] Приложение С1 «Соглашение ТРИПС»
[5] Приложение С1 «Соглашение ТРИПС»
[6] Документы ВОИС скопированы с официального сайта ВОИС www.wipo.org
[7] Парижское Соглашение 1967г.

«торговые аспекты», а скорее «имеющие отношение к торговле», выделяет следующие объекты, посвящая каждому определённый раздел:

- Авторское право (ст. 9-14);
- Торговые марки (ст.15-21);
- Географические указания (ст.22-24);
- Промышленные образцы (ст.25-26);
- Патенты (ст.27-34);
- Интегральные микросхемы (ст.35-38);
- Торговые секреты (ст.39).

Открывающая Часть II и раздел «Авторское право» статья 9 содержит положение о том, что «Участники должны соблюдать статьи 1-21 Бернского соглашения 1971 года». Указанные статьи содержат базовые понятия и принципы авторского права. Сроки на охрану смежных прав установлены в 50 лет.

Для промышленных образцов срок охраны установлен в течение 10 лет.

Одной из причин, по которой многим странам приходится корректировать своё законодательство при подписании пакета ВТО, это положения раздела, касающегося патентов (ст.27-34).

Значительно ограничивается возможность широкого общественного доступа к запатентованной продукции в некоторых областях производства. В частности, в некоторых странах упразднены законы, запрещающие патентование в фармацевтической и сельскохозяйственной сфере. Ограничивается возможность обязательного лицензирования. Срок охраны патента устанавливается, согласно статье 33 Соглашения, 20 лет со дня регистрации.

Защита топологий интегральных микросхем, или, как их ещё называют, чипов, основана на положениях Вашингтонского Соглашения по Охране топологий интегральных микросхем 1989г[8]. Основное отличие заключается в увеличении срока защиты с 8 до 10 лет.

Соглашение по ТРИПС так же охраняет такой объект, как торговые секреты. Этот объект обладает многими признаками интеллектуальной собственности, однако причисление его к таковым может вызвать споры. Тем не менее, Соглашение в статье 39 обязывает страны участницы обеспечить защиту торговых секретов, кроме случаев, когда это противоречит честной коммерческой практике.

Исполнение условий, предусмотренных в I и II частях, для России, в случае подписания Соглашения, не составят большого труда. Россия является участницей соглашений под эгидой ВОИС, которые, в некоторых вопросах стали основой соглашения по ТРИПС. Сложности вызывают положения части III «Осуществление прав интеллектуальной собственности» (ст. 41-61). Сложности начинаются сразу – со статьи 41, которая требует со стороны участников гарантий оперативного предотвращения любых нарушений прав

[8] Вашингтонская Конвенция о защите топологий интегральных микросхем 1989г.

интеллектуальной собственности. Это, естественно, должно быть отражено как на уровне законодательства, так и на организационном уровне.

Часть IV посвящается приобретению права интеллектуальной собственности. Здесь предусматривается доступность и простота процедуры регистрации, совместимой с целями Соглашения для объектов, которым посвящена часть II.

ВТО основывается на иных принципах, чем ВОИС, и в сложившейся ситуации должна иметь место определённая конкуренция юрисдикции двух международных организаций. Проблему разграничения поможет определить рассмотренное ниже, подписанное в 1995году *Соглашение о сотрудничестве ВОИС и ВТО*[9].

Международное Бюро ВОИС должно гарантировать предоставление копий нормативных актов, инструкций, имеющихся в наличии переводов, компьютерных баз данных Секретариату ВТО, совету по ТРИПС, участникам соглашения о создании ВТО и их подданным, на тех же условиях и в те же сроки, как это было бы сделано для членов ВОИС и их подданных. В свою очередь, ВТО и совет по ТРИПС должен предоставить аналогичные услуги. Пункт «а» части 3 статьи 2 Соглашения между ВТО и ВОИС имеет ссылку на пункт 2 статьи 63 Соглашения по ТРИПС, которое предусматривает, что член ВТО освобождается от обязанности сообщать Совету по ТРИПС о тех решениях суда, инструкциях, мерах, связанных с защитой ИС внутри государства-члена (эти сообщения необходимы для обзора деятельности в рамках Соглашения), если эти решения были переданы, в ходе консультаций, в регистр Международного Бюро ВОИС. Так же в этом пункте предусматривается, что, когда член ВТО сообщает в Совет по ТРИПС о появлении нового документа в регистре ВОИС, Секретариат имеет право обратиться в международное бюро ВОИС о безвозмездной передаче копии такого документа.

Помимо вопросов, предусмотренных данным соглашением, сотрудничество ВОИС и ВТО реализуется в совместных программах. В частности, с 2001 года введена в действие совместная программа помощи развивающимся странам по вопросам интеллектуальной собственности[10].

Из всего вышесказанного можно сделать вывод, что опыт правового регулирования ИС, информационная база, приобретённые за долгие годы деятельности ВОИС, делают необходимым сотрудничество двух организаций. ВОИС в перспективе, возможно, возьмёт на себя роль гуманитарно-просветительской и консультативной организации, сегодня её деятельность так же необходима, как и раньше. Появление Соглашения по ТРИПС свидетельствует о развитии как международного права, так и права интеллектуальной собственности, что требует более чёткого юридического разделения сфер межгосударственного регулирования на экономическую и гуманитарную по вопросам интеллектуальной собственности.

---

[9] Соглашение о сотрудничестве ВТО и ВОИС. Скопировано с официального сайта ВОИС www.wipo.ru

[10] Доклад проф. М.Вальтера на семнадцатой очередной сессии Межправительственного комитета Римской конвенции.

2.3. Организация системы промышленной и экономической контрразведки в инновационных организациях

Если задачи выведывания военных секретов и политических планов противника испокон веков стояли во главе деятельности любой самой примитивной разведки, то и своего рода промышленный шпионаж всегда играл не меньшую роль. В детстве многие зачитывались книгой «Борьба за огонь» о том, как одно доисторическое племя охотилось за секретом другого, овладевшего умением добывать огонь. Секреты выделки шкур, изготовления луков или копий — все становилось объектом шпионажа. Моисей и другие библейские вожди засылали своих разведчиков в тыл врага «вызнавать все о земле, ее плодородии, богатствах». Хорошо поставленную службу промышленной разведки имел древний Рим: он собирал подробные сведения о своих соседях и потенциальных противниках по многим экономическим аспектам, в том числе о климате, состоянии дорог, плодородии земель, трудолюбии населения, наличии продовольственных запасов, о местах хранения и объемах сокровищ, накопленных церквями и правителями. Все эти сокровища выявлялись разведкой и впоследствии оказывались в «сейфах» Римской империи. Не случайно нынешним ученым не попадаются клады римской эпохи — есть более ранние или более поздние, а этих нет. Шпионы римского императора Юстиниана — странствующие персидские дервиши — раскрыли секрет производства шелка, привезя из Китая шелковичных червей в полостях своих посохов. В свою очередь и японцы послали в Китай официальную делегацию якобы с целью пригласить китайских мастеров по производству шелка в Японию, хотя заведомо знали, что им откажут. Делегация провела при дворе китайского императора столько времени, и вела себя так умело, что выведала все секреты, и вскоре Япония стала производить свой шелк. Но подлинным создателем экономического и военно-промышленного шпионажа можно, пожалуй, назвать Чингисхана. Ни одного похода он не предпринимал без изучения экономической обстановки на территории будущего противника: природных богатств, наличия полезных ископаемых, уровня развития ремесел и военного дела, сокрытых сокровищ, богатых могильников. Не без помощи шпионов в руки Чингисхана и его ближайших наследников попали огромные богатства Аббасидов, сокровища китайских царей и багдадских халифов, золото исидов. Своеобразным был подход Чингисхана к тому, что ныне называют «ноу-хау». Почти поголовно уничтожая население завоеванных городов, он сохранял жизнь мастерам, оружейникам, златокузнецам, архитекторам и другим людям, владевшим тайнами ремесла; более того, он установил закон: учиться у всех народов всему лучшему, что те создали. В XVIII веке началась охота за «китайским секретом» — способом производства фарфора. В Китай засылали множество шпионов, и первым из них, преуспевшим в этом деле, стал французский монах-иезуит. Ему удалось проникнуть в закрытый город Цзиндэчжэнь, где находилась императорская фарфоровая мануфактура. Он детально изучил технику производства твердого фарфора из каолина и, несмотря на бдительность китайской контрразведки, сумел отправить во Францию образцы сырья.

Некоторое время спустя там началось производство знаменитого севрского фарфора. В свою очередь, английский агент Томас Бриан, работавший в Севре, похитил у французов технологию производства фарфора, и вскоре она была запатентована в Англии! Надо сказать, что немецкими химиками (точнее, алхимиком Фридрихом Бётгером) секрет производства фарфора был открыт самостоятельно в начале XVIII века и погоня за секретом саксонского фарфора была не меньшей, чем за китайским. Бётгер так тщательно берег свою тайну, что, кроме него, ее никто не знал: по его настоянию половину рецепта выучил наизусть ученый Немиц, вторую половину - Гартельмей. Можно смело утверждать, что в течение целого столетия фарфор был главной мишенью шпионажа. Но, естественно, охота шла и за другими производственными секретами. Английский литейщик Фомо, находя английскую сталь того времени низкокачественной, переодевшись в лохмотья, под видом странствующего скрипача отправился на континент, где, посетив все европейские сталелитейные центры, сумел выкрасть секреты производства лучших сортов стали. Вскоре его заводы сделались крупнейшими в Англии. Он умер богатым человеком, а его дети получили дворянский титул. Далеко не все промышленные секреты приходилось добывать с неимоверным трудом. Например, изобретение пороха приписывается немецкому монаху Бертольду Шварцу, жившему в XIV веке, в то время как секрет его производства был почти одновременно похищен или куплен без особого труда рядом европейских шпионов у мусульман и китайцев. Так же легко были похищены у арабских алхимиков все секреты производства кислот.

Шли годы и десятилетия, объектов для промышленного шпионажа все прибавлялось. Постепенно он становился «узаконенным». Так, декрет французского правительства 1791 года, признававший «за всяким, кто первый привезет во Францию какой-либо иностранный промысел, такие же льготы, какими пользовался бы его изобретатель», фактически явно поощрял промышленный шпионаж. В конце XVIII века в Манчестере возникла ассоциация борьбы с патентами и монополиями. Вероятно, это была первая всемирная организация, поощрявшая промышленный шпионаж. Постепенно, поддерживаемый государством и промышленниками, он превращался в важный фактор как промышленной революции, так и политики. В шпионаж вовлекались все новые лица, и среди них не только платные шпионы, но и ученые с мировым именем.

Очень эффективным был (и остается) японский промышленный шпионаж, поставленный на государственную основу. У многих существует ложное представление, что скачок японской индустрии начался лишь после Второй мировой войны. Однако это не так. С конца XIX века Япония вступила на путь индустриализации. Всеми правдами и неправдами она стремилась догнать передовые страны. Первое время японцы выманивали промышленные секреты, обещая размещать заказы, но вскоре эту их уловку раскрыли. Поводом для разоблачения послужил занятный инцидент. Японцы попросили ознакомиться с устройством одного насоса, обещая сделать большой заказ. По случайности, в образце, который им был предложен, имелся дефект — дыра в

цилиндре, соответствующим образом заделанная болтом с двумя гайками. Японцы скопировали насос буквально в таком виде, как его осмотрели, то есть с болтом и гайками. Этот случай получил широкую известность, и японцы заслуженно приобрели репутацию «поделыциков». Однако японские шпионы и ученые продолжали усиленно работать, воруя чужие секреты, внося коррективы в производство, совершенствуя старое и изобретая новое. Вскоре они освоили изготовление бездымного пороха, торпед, новейшие способы литья стали, технику электрических прожекторов большой мощности. Добыв с помощью шпионажа секрет производства высококачественных оптических линз, японцы выбросили на рынок фотоаппараты высокого качества по внеконкурентным ценам. То же произошло с виски и велосипедами. Начиная с 1910 года надпись «Сделано в Японии» стала символом высококачественного и дешевого товара. К этому времени японские покупатели, туристы, студенты заполонили европейские и американские города, и каждый, как пчела в улей, тащил в Японию новые и новые промышленные секреты, тем более что японский кодекс нравственности и быта, известный под названием «Бу-сидо», вменяет в обязанность каждого японца шпионаж в пользу монарха и государства, считая такое занятие проявлением долга и чести. Было бы наивно пытаться даже просто перечислить все изобретения или методы производства, похищенные в XIX и XX веках.

Пожалуй, нет ни одного более или менее стоящего объекта военной или гражданской промышленности, который не стал бы предметом внимания иностранных разведок. Задачами шпионажа становились не только получение уже завершенных изобретений, формул и методов, но и выявление изобретения в самой начальной его стадии, заявок на получение патентов, изобретателей и мелких лабораторий, терпящих финансовые затруднения и позволяющих затем использовать их в своих интересах, завладение секретами «ноу-хау» (вспомним Чингисхана), организация «утечки мозгов» и целый ряд других грязных и хитроумных методов. Борьба с ними велась зачастую не менее изощренными способами, которые и стали прообразом промышленной контрразведки. Одним из государственных деятелей, особенно поощрявшим промышленный шпионаж, был Наполеон. Он объявил нечто вроде конкурса и предложил ряд премий за изготовление (любым методом — похищением или изобретением) лучших сортов стали.

Как ни парадоксально, победителем стал молодой немец Фридрих Крупп, купивший у шпионов несметное число секретных формул, сталь заводов которого впоследствии не раз нанесет огромные потери Франции и ее народу. Так он использовал премию Наполеона. Об истории империи Круппа, полной драматических и трагических событий, в которой громадную роль сыграли шпионы той или другой стороны, написаны многие тома и пересказывать ее нет никакой возможности. Мы же вспомним его потому, что сына Ф. Круппа — Альфреда можно смело назвать отцом организованной промышленной контрразведки. Приняв наследство отца с отрицательным балансом, Альфред Крупп сам занялся шпионажем и вскоре разбогател, овладев рядом производственных секретов. Вводя их на своих заводах, он поставил перед

собой задачу: сделать так, чтобы они не были похищены. Поэтому он страстно увлекся делом промышленной безопасности. Он просил прусское правительство обязать рабочих присягать ему в особой верности и лояльности. Ему отказали, но это не помешало Круппу заставлять приносить ему присягу не только рабочих, но и шпионов, засылаемых к конкурентам. Он подозревал всех. Своему брату он послал служебную записку: «Я подозреваю ночного сторожа. Он часто бывает на работе днем». А. Крупп успешно выполнил свою программу — максимальный внешний шпионаж и доведенная до крайности внутренняя безопасность. В 1872 году Крупп опубликовал и раздал рабочим правила внутреннего распорядка, чем впервые была легализована современная промышленная безопасность. Одна из фраз этих правил гласила: «Независимо от издержек производства необходимо, чтобы за рабочим постоянно наблюдали энергичные и опытные люди, которые получали бы премию всякий раз, когда задерживали саботажника, лентяя или шпиона». С годами контрразведка империи Круппа совершенствовала свою деятельность. Именно она разработала бесчеловечную технику облучения посетителей (без их ведома) большой дозой икс-лучей, которые засвечивали фотопленку, вызывая в то же время серьезные физические расстройства. Шпиономания и преследование инакомыслящих на заводах Круппа дошли до предела. С 1933 по сентябрь 1939 года 700 служащих Круппа были отправлены в концентрационный лагерь. В 1945 году в подвале бюро Густава Круппа в Эссене союзники обнаружили камеру пыток. Расследование показало, что служба промышленной безопасности Круппа подвергала пыткам лиц, подозреваемых в шпионаже, и хоронила их трупы на территории завода. Все эти зверские меры привели к тому, что за пределы фирмы Круппа не ушел ни один секрет.

Все упомянутые выше методы относились скорее к пассивной защите секретов и проведению мер промышленной безопасности. Однако уже и в те далекие времена находились специалисты, считавшие, что задачей промышленной контрразведки является в первую очередь введение противника в заблуждение и профилактика. И в этом деле Крупп оказался на высоте. В 1920 году он основал в Эссене бюро, занимавшееся промышленным шпионажем и камуфляжем. Оно, в частности, сумело похитить у французов конфискованную после войны гигантскую пушку, стрелявшую по Парижу в 1918 году, и закамуфлировать ее в гигантской заводской трубе (вспомним, что это было время, когда Германии было запрещено иметь и производить тяжелое вооружение). Некоторыми фирмами предпринимались довольно наивные методы введения в заблуждение вражеских шпионов. К примеру, одна французская компания по производству шин изменила градуировку на шкалах всех термометров, использовавшихся в производственном цикле. Ряд компаний по рекомендации контрразведки стал нанимать специалистов, вносящих в схемы или формулы, которые могли заинтересовать противника, незначительные изменения, но такие, после которых информация уже не стоила ни гроша, а шпионы продолжали добросовестно снабжать ею пославшую их правительственную или частную организацию.

Хотелось бы, привести выдержку из заявления руководителя французской организации промышленной контрразведки «ПСИ» полковника Барраля, бывшего сотрудника спецслужб: «Проблемы безопасности надлежит ставить на уровне той власти, которая может их разрешить. Неэффективность систем безопасности многих французских предприятий, искренне убежденных, что они защищены от промышленного шпионажа, объясняется тем, что они не организовали защиту информации на надлежащем уровне. Люди, отвечающие за безопасность, часто плохо подготовленные или совсем не подготовленные к такой работе, изолированы от важных служб, деятельность которых им неизвестна, являются в глазах персонала полицейскими, а в глазах дирекции бременем, хотя их работа плохо оплачивается. В конце концов они мирятся с этим подчиненным положением, и тогда их работа ограничивается некоторыми поверхностными обследованиями или составлением памятных записок, с которыми никто не считается. Находясь в таком второстепенном положении, они, как правило, последними узнают об утечках информации, если вообще узнают о них. Никогда не имея возможности сделать анализ положения с информацией на предприятии, они не знакомы с путями ее следования и не располагают к тому же ни властью, ни средствами, а порой и техническими знаниями, необходимыми для предотвращения новых утечек. Безопасность — новая наука, которую должны были бы изучить все директора. Это новая функция в промышленности, и ее место в правлении, а не в кабинете человека, которому поручено обследование, или начальника охраны».

Сегодня роль промышленной разведки возросла многократно и охватывает все составляющие мировой экономики. Общеизвестно, что 90% секретной информации можно найти в открытых источниках, но для этого надо уметь искать и анализировать полученную информацию. На занятиях студенты научатся искать источники информации, «подбирать к ним ключи», обрабатывать информацию и пользоваться ею в интересах своей компании.

Появление контрразведки было обусловлено необходимостью защитить свои секреты от чужих глаз и ушей. Это труднейшая задача, которая посильна только хорошо подготовленным профессионалам. С каждым годом конкуренция во всех сферах человеческой деятельности растёт, и очень многие частные лица и компании стремятся завладеть чужими секретами без разрешения их владельцев. Ущербы от этого настолько велики, что в структуре всех серьёзных компаний имеются контрразведывательные подразделения.

Контрразведывательная деятельность в сфере бизнеса заключается в следующем:

- выявление потенциальных противников, их разведывательного и подрывного потенциала;
- выявление агентуры противника и потенциальных предателей (неустойчивых лиц) среди персонала фирмы;
- мероприятия по маскировке своей коммерческой, разведывательной и контрразведывательной деятельности, в том числе и активная дезинформация;

- вербовка агентуры в лагере противника, внедрение туда своих секретных сотрудников;
- активное противодействие противнику (в частности, секретным сотрудникам и агентам его разведки, а также хакерам, подрывникам, киллерам)

Методика оперативного планирования контрразведывательной деятельности рекомендует начинать работу с сортировки имеющихся задач по порядку их значимости и сложности. В данном аспекте - это необходимость выделить из общего частного - главное.

Анализ имеющихся версий начинается с отработки всех возможных простейших объяснений происшествия и только затем необходимо переходить к чему-то более сложному. Разбитая на мелкие части большая проблема Ч всегда решается намного легче. Работу контрразведки можно сравнить с восхождением по длинной лестнице, постепенно и снизу - вверх, а не запрыгивая сразу же на верхнюю планку.

Большое значение в работе контрразведки по фактическому подтверждению версии имеет метод подбора и сопоставления фактов. 99,9% времени у контрразведчика уходит на то, чтобы смотреть, слушать, сопоставлять и анализировать.

Один безобидный факт, возможно, ничего и не значит, но если к нему добавить большое количество других, в такой же степени безобидных, фактов, то количественное очень часто переходит в качественное. Как антрополог по частичкам сохранившего скелета воссоздает внешний вид давно вымерших динозавров, так и грамотный контрразведчик из большого количества тщательно отобранных и проанализированных фактов может составить определенное мнение об интересующем его вопросе.

Естественно, что получить информацию о готовящемся или уже имеющемся проникновении на предприятие разведорганов конкурентов невозможно без использования конфиденциальных источников.

Большим подспорьем в работе Службы безопасности инновационного предприятия является создание единого интегрированного банка данных (далее ИБД), где бы накапливалась вся информация, поступающая в СБ, как из открытых, так и конфиденциальных источников.

Для эффективного использования ИБД Службы безопасности необходимо тщательное информационное моделирование ее предметной области. Для проведения качественной информационно-аналитической работы требуется разноплановая информация, характеризующая различные взаимосвязанные аспекты анализируемой проблемы. Также требуются данные о структуре решаемой задачи, которая должна, как мозаику, соединить между собой различные информационные фрагменты и образовать максимально приближенную к реальности полную и целостную картину предметной области. Поэтому разработчик структуры ИБД должен хорошо себе представлять модели источников внешних и внутренних угроз предприятию и вероятностных связей объектов учета между собой. Модель предметной области ИБД должна включать в себя такие информационные объекты, как

"Организация", "Лицо", "Адрес", "Телефон", "Автотранспортное средство", "Реферат о событии", "Договор", "Переговоры" и т.д. При этом необходимо учитывать не только многообразие связей и отношений между объектами учета, но и тот факт, что информация об одних и тех же объектах поступает из разных источников и в разное время, имея при этом ситуационный характер в виде высказываний о совокупности взаимосвязанных объектов.

В настоящее время на многих предприятиях разработаны и успешно эксплуатируются ИБД, где модель предметной области обладает достаточной эволюционной самостоятельностью и позволяет организовать интеграцию (взаимное дополнение) разнородных сведений по одним и тем же объектам (лицам, фирмам, адресам, телефонам, автотранспортным средствам) путем их идентификации и слияния по мере поступления новых данных. Таким образом, при введении новых объектов происходит установление связей между ними и уже имевшимися объектами, а также дополнение уже имевшихся объектов новыми характеристиками. В результате наращивается сетевая структура связей объектов и образуется «производная» информация, не вводившаяся в явном виде в банк данных, становится возможным проследить цепочки взаимосвязанных объектов, выражающих признаки рисковых ситуаций. В условиях такого описания структуры предметной области достаточно выйти на один информационный объект, чтобы по связям исследовать его окружение. В качестве примера рассмотрим выявления с помощью ИБД мошенников, взяточников или агентуры конкурентов. Разработка объекта оперативного интереса (далее ООИ) должна начинаться с выявления и внесения в ИБД всех родственных, деловых и дружеских связей объекта. Идея интеграции этих сведений состоит в том, что, если в процессе работы лицо или адрес раньше появлялись по другому сообщению, система при закладке информации вторично, сама, без какой-либо команды со стороны пользователя, сливает по указанным объектам учета, что было, и то, что внесено в данный момент. Как раз при таком слиянии образуются и наращиваются цепочки причинно-следственных связей.

При закачке разнородной информации, именно на ее стыках и получаются самые интересные вещи. Допустим, сливается база данных отдела кадров, база данных регистрационных органов, из текстовых файлов заносится информация о рекламе, в результате дальнейшей информационно-поисковой работы контрразведки по подтверждению информации ИБД отрабатывается ряд моделей возможных связей ООИ. Далее мы остановимся на этом более подробно. Одним из наиболее качественных и надежных каналов выявления на предприятии мошенников, взяточников или агентуры конкурентов является контроль над доходами и расходами его сотрудников, имеющих право финансовой подписи или допущенных к конфиденциальной информации. Появление у объекта оперативного интереса контрразведки сумм, не отраженных в его налоговой декларации, должно стать сигналом к проведению мероприятий по установлению источников его непомерно возросших доходов.

Обычно получив легкие и быстрые деньги, люди тратят их, не задумываясь. Это выражается в оплате старых долгов, покупке дорогих

автомашин, отпускных заграничных вояжах и крупных подарках женам и любовницам.

Любые изменения в жизненном цикле объекта, будь то немотивированное изменение сексуального поведения, частые посещения ресторанов, эксклюзивная одежда и модельная обувь, являются сигнальной информацией для контрразведывательного подразделения СБ. По учетам налоговой инспекции необходимо установить совокупный годовой доход ООИ и его учредительство в коммерческих или некоммерческих организациях (данную информацию также можно получить и в органах государственной регистрации), возможно также, что объект может быть зарегистрирован как предприниматель без образования юридического лица.

В обязательном порядке должны быть отработаны родственные связи объекта. Очень часто при покупке различного оборудования или при оказании каких-то услуг лицу, от которого зависит лоббирование данного вопроса, предлагается определенный процент от суммы заключаемой сделки. Наиболее часто это происходит при больших объемах закупок или при оказании страховых услуг. Так, например, такса за страхование в конкретной страховой компании составляет 10% от страховой премии страхователя. Иногда разоблачить корыстного служащего достаточно просто: сумма ежемесячной зарплаты его жены в страховой компании с точностью до копейки составляет ровно 10% от сумм, перечисленных туда предприятием.

Домашние адреса и телефоны ООИ и его родственников должны быть проверены по различным учетам (регистрационная палата, налоговая инспекция, фонд медицинского страхования, пенсионный фонд и т.д.) на предоставление их в качестве юридических или фактических адресов коммерческих организаций или их контактных телефонов. Очень большие возможности в этом направлении дает отработка рекламных объявлений (т.е. занесение в ИБД информации об адресах и контактных телефонах различных организаций) и установление их связей с адресами и телефонами сотрудников предприятия. Также в отдельную базу данных ИБД должны заноситься данные о служебных командировках объекта: место, время, задание на командировку, кто посылал, с кем объект ездил в командировку и с кем там имел дело.

Под контроль должны быть взяты все переговоры со служебного телефона объекта, с фиксацией номера телефона абонента, времени разговора и, по возможности, самой беседы. Все данные также должны заноситься в базу данных "Телефон" ИБД.

Все договоры предприятия должны заноситься в базу Договор с фиксацией их инициаторов. В базе данных "Переговоры" необходимо фиксировать: кто вел переговоры, кто участвовал в их подготовке, по чьей инициативе они проходили, какая тематика обсуждалась, не имели ли участвовавшие в переговорах контрагенты неформальных контактов с отдельными сотрудниками предприятия, каковы интересы контрагентов на рынке.

Одним из эффективных приемов работы контрразведки является недопущение узурпации единоличного заключения финансовых договоров кем-

нибудь из топ-менеджеров. В состав подразделений или групп, участвующих в заключении договоров, должны также включаться и сотрудники Службы безопасности предприятия, работающие под прикрытием. Это эффективно с двух позиций, во-первых, идет квалифицированный сбор информации о партнере и его возможных криминальных устремлениях к предприятию и его сотрудникам, а также осуществляется профилактическая отработка возможных негативных связей сотрудников предприятия. Цепочка связей по адресам, телефонам, совместным командировкам, проведенным переговорам и заключенным договорам может привести к очень интересным выводам в виде достаточно разветвленной причинно-следственной цепочки. Для решения задач данного класса обычно используется инструментальная система управления базами данных.

Используя описанную выше методику, Служба безопасности предприятия по разрозненным данным из различных источников имеет возможность отследить и оценить кризисную ситуацию до того, как она станет достоянием всеобщей гласности, а также разработать оптимальную антикризисную программу, что является важным фактором конкурентной борьбы, дающим предприятию прямой экономический эффект.

Однако стоит еще раз напомнить, что при выявлении признаков готовящегося или совершенного преступления подразделение экономической контрразведки предприятия должно осуществлять тесное взаимодействие с органами внутренних дел, ФСБ и прокуратуры.

ГЛАВА 3. РАЗРАБОТКА ПОЛИТИКИ СУБЪЕКТА ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основные положения политики информационной безопасности в инновационных организациях

Зарубежный и отечественный опыт обеспечения безопасности инновационной деятельности свидетельствует, что для борьбы со всей совокупностью потенциально возможных угроз, связанных с конфиденциальной информацией, защитой ноу-хау и поддержанием конкурентоспособности хозяйствующего субъекта, необходима стройная и целенаправленная организация процесса противодействия. Причем в организации этого процесса должны участвовать не только люди, ответственные за это направление, но и специалисты в области защиты информации, руководство организации, ведущие сотрудники организации. Для этого необходимо разрабатывать для каждой конкретной организации свою политику информационной безопасности.

Целью разработки политики субъекта инновационной деятельности в области информационной безопасности является определение правильного (с точки зрения организации) способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности.

Политика информационной безопасности хозяйствующего субъекта выражает систему взглядов на проблему защиты конфиденциальной информации и коммерческой тайны, раскрытие которых может привести к серьезным прямым убыткам и полной потере конкурентоспособности на различных этапах и уровнях предпринимательской деятельности, а также основные принципы, и направления реализации мер информационной безопасности.

Политика безопасности субъекта инновационной деятельности определяется в изданном специальном документе (или своде документов), в котором рассматриваются вопросы философии, задач, организации, стратегии, методов в отношении обеспечения конфиденциальности, целостности, доступности информации и информационных ресурсов предприятия.

Философия определяет подход к организации информационной безопасности предпринимательской фирмы, структуру и руководящие принципы информационной стратегии безопасности. Философию безопасности можно представить, как большой купол, под которым находятся все другие механизмы безопасности предприятия. Философия должна объяснять во всех будущих ситуациях, почему предпринимаются те или иные действия при обеспечении защиты информации.

Задачи политики информационной безопасности направлены на реализацию назначения (целей) систем защиты и основных функциональных

требований, предъявляемых к информационным ресурсам коммерческой структуры.

Этап формирования требований к безопасности информационных ресурсов является принципиально важным при выработке политики информационной безопасности. От качественного проведения этого этапа в определенной степени зависит уровень всех дальнейших проектных решений по защите информации и, в конечном итоге, достигаемый уровень безопасности коммерческой фирмы в целом.

Если требования к безопасности в начале разработки политики предъявлены не в полной мере, то результирующая политика может не отвечать своему предназначению.

Для формирования требований к безопасности должны быть учтены все факторы, определяющие условия функционирования системы безопасности, возможные угрозы, а также стандартные каталоги требований.

Исходным пунктом для формирования требований является установление среды информационной безопасности. При определении среды безопасности необходимо учитывать:

1. Физическую среду, которая определяет все аспекты внешней среды, имеющие отношение к безопасности, включая условия физической безопасности защищаемого объекта, нормативно-правовую базу и данные, относящиеся к персоналу.
2. Информационные активы, подлежащие защите, к которым должны применяться требования и меры безопасности.
3. Назначение защищаемого объекта, в том числе, технические характеристики и область применения аппаратных и программных средств.

Анализ факторов внешней среды завершается описанием следующих параметров среды безопасности:

- Угроз безопасности, которые могут быть реализованы по отношению к защищаемому объекту. В описании угроз безопасности должны содержаться следующие компоненты:
  - Источник угрозы.
  - Способ реализации.
  - Уязвимости объекта, которые могут быть использованы для реализации угроз.
  - Ресурсы, подверженные действию угроз.
- Мер и правил политики безопасности организации, которые обеспечиваются по отношению к объекту защиты. Такие меры конкретно формулируются, а для универсальных объектов делаются общие утверждения в отношении политики информационной безопасности организации;
- Предположений об условиях, которые должны быть обеспечены в среде, чтобы объект мог рассматриваться как безопасный.

Для установленной среды безопасности объекта оцениваются риск и возможный ущерб от нарушения безопасности, являющиеся исходными данными для определения мер и средств противодействия, которые должны быть реализованы при защите, а также их эффективность.

При разработке положений по установлению среды безопасности целесообразно учесть модель безопасности ГОСТ Р ИСО/МЭК 15408, которая изображена на рис. 5.

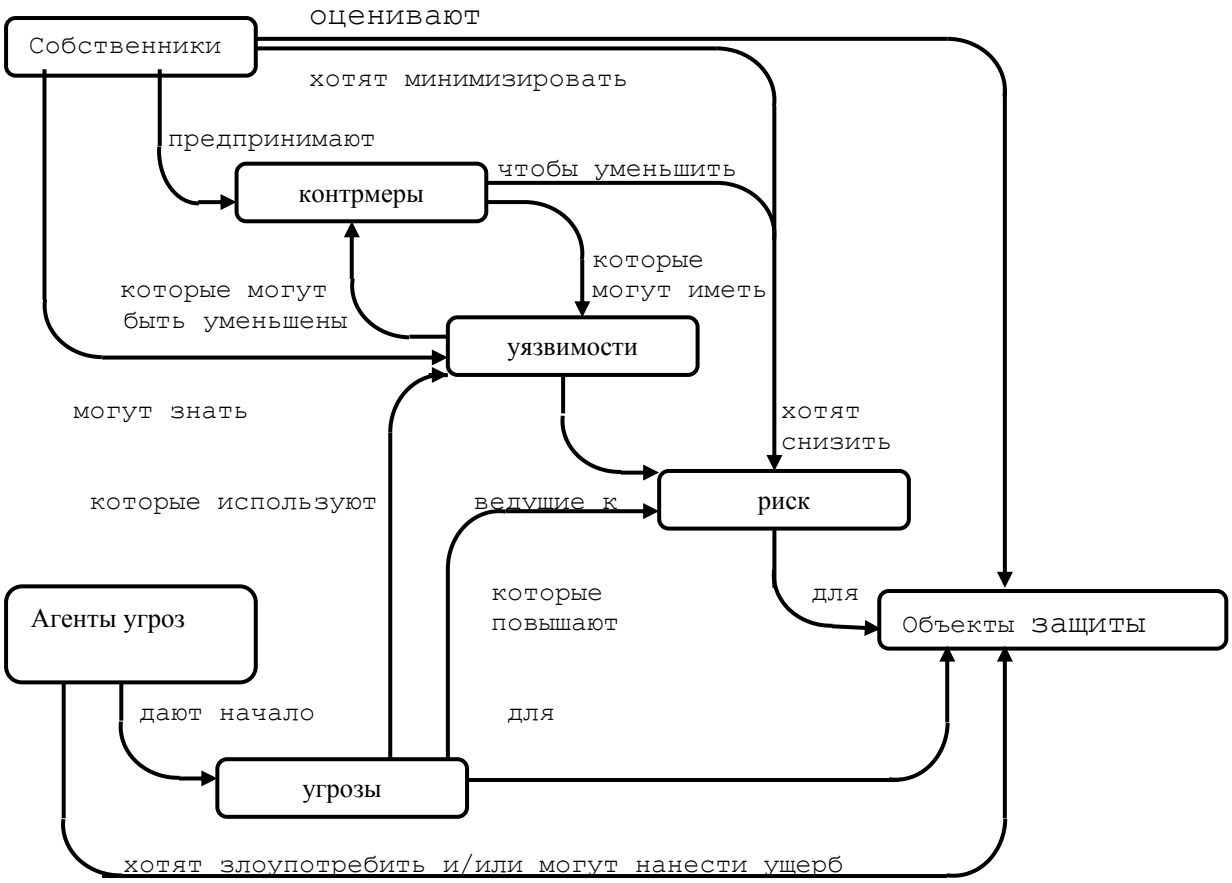

Рис.5. Модель безопасности по ГОСТ Р ИСО/МЭК 15408.

Результаты анализа среды безопасности предназначены для формулирования целей безопасности защищаемого объекта, направленных на противодействие выявленным угрозам безопасности и соответствующих политике безопасности организации и условиям, определенным для среды безопасности. Необходимость определения целей безопасности состоит в том, чтобы выразить все намерения в отношении обеспечения безопасности объекта и определить, какие из них будут обеспечиваться средой безопасности.

Требования безопасности представляют собой результат преобразования целей безопасности в совокупность требований по защите объекта и требований безопасности для его среды, которые в случае их выполнения, обеспечивают уверенность, что выработанная политика информационной безопасности отвечает целям безопасности организации в целом.

В итоге, формирование требований к защите объекта при разработке политики информационной безопасности можно изобразить следующим образом (рис.6):

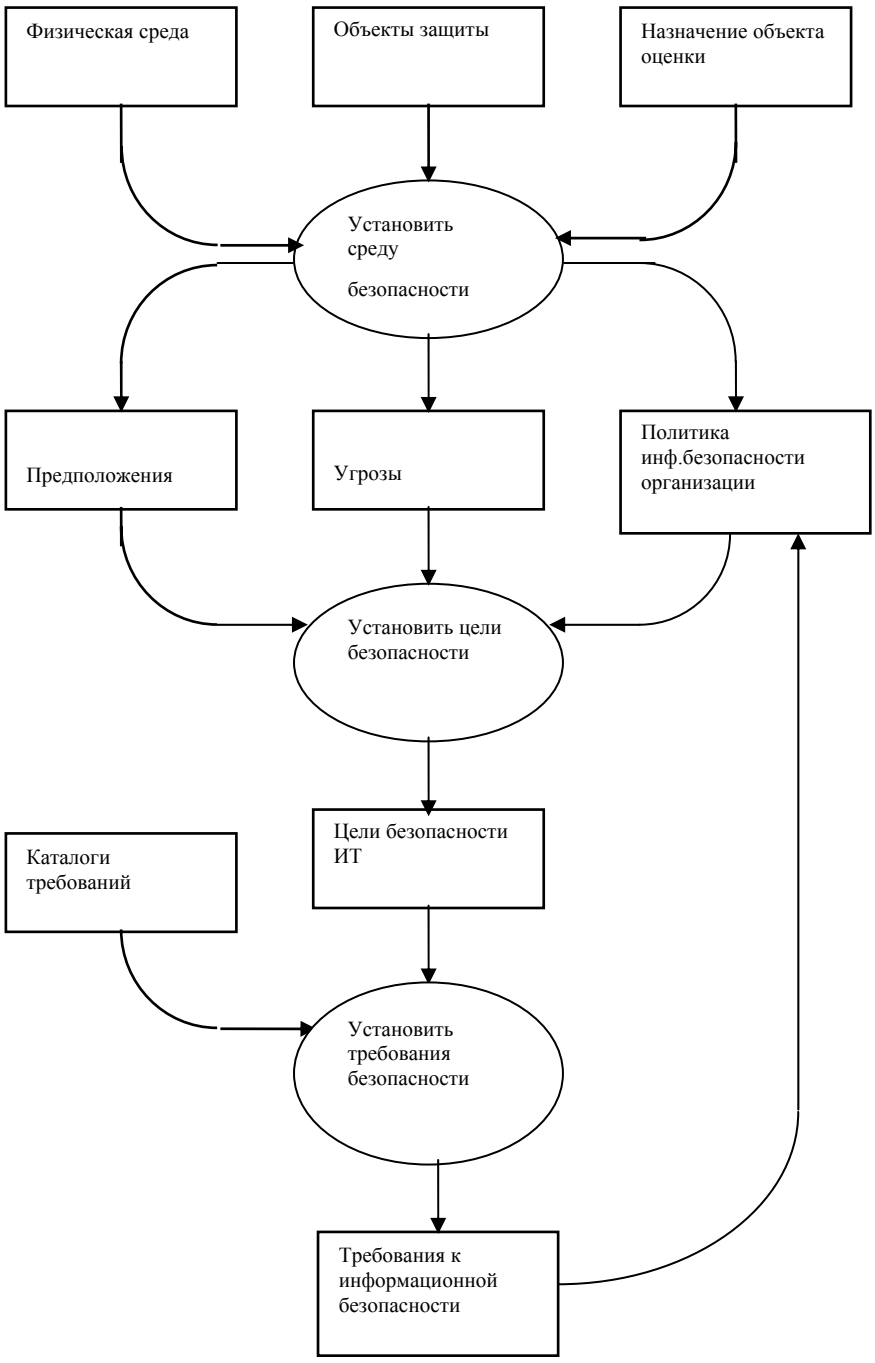

Рис.6. Формирование требований к защите объекта при разработке политики информационной безопасности хозяйствующего субъекта.

Политика информационной безопасности субъекта инновационной деятельности отражает стратегию управления в отношении защиты информации.

В данном случае стратегия представляет собой план или проект в философии безопасности. Детализация этого плана показывает, как организация намеревается достигнуть целей, поставленных в пределах структуры философии, и какие методы применять в каждом конкретном случае.

Определение целей системы защиты информации включает следующие пункты:

- Определение необходимого с точки зрения экономической целесообразности уровня информационной безопасности хозяйствующего субъекта.
- Определение методов достижения необходимого уровня защищенности оптимальным сочетанием технических средств по основным направлениям проведения работ и организационных мер.
- Определение этапов создания системы защиты информации хозяйствующего субъекта.

Рекомендации по внедрению конкретных методов защиты информации для реализации политики безопасности содержат:

- Обзор мер защиты, позволяющих реализовать комплекс защиты на защищаемых объектах, включающих организационные мероприятия, технические средства, программно-аппаратные средства.
- Предложения и рекомендации по выбору и размещению на объекте основных средств защиты.
- Разработку технико-экономического обоснования внедрения системы информационной безопасности, оценку эффективности данной системы с учетом оценки вероятности возможных угроз и величины возможных потерь;
- Разработку плана по реализации и поддержанию политики информационной безопасности.
- Разработку предложений по совершенствованию и развитию системы защиты информации на предприятии.
- Оценку ожидаемой эффективности предлагаемых мер защиты с учетом эффективности, стоимости, бесконфликтности с используемым на объекте программным обеспечением, простоты эксплуатации.

Политика безопасности предприятия должна отвечать на три главных вопроса:

- Что защищать?
- От кого (от чего) защищать?
- Как защищать?

Отвечая на первый вопрос, важно отметить, что реализацию жизненно-важных интересов любого субъекта инновационной деятельности обеспечивают его корпоративные ресурсы, особенно ресурсы, содержащие ценную информацию, разглашение которой может привести к значительному, а иногда, к не поправимому ущербу конкурентоспособности субъекта предпринимательской деятельности. Эти ресурсы должны быть надежно защищены от прогнозируемых угроз. Для предпринимательской структуры такими важными для жизнедеятельности ресурсами, а следовательно, предметами защиты являются:

- Конфиденциальная информация:

На материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи, в кабинетах руководства предприятия, на совещаниях и заседаниях;

- Финансово-экономические ресурсы:

Обеспечивающие эффективное и устойчивое развитие хозяйствующего субъекта (коммерческие интересы, бизнес-планы, договорные документы, обязательства и т.п.)

- Имущество:

Секретная и конфиденциальная документация, интеллектуальная собственность (ноу-хау), ценная информация, содержащаяся на магнитных носителях и т.д.

- Персонал предприятия:

Люди, допущенные в особо важные точки (ОВТ) предприятия, владеющие конфиденциальной информацией.

Для обеспечения защиты интеллектуальной собственности, сведений, составляющих коммерческую тайну на хозяйствующем субъекте вводится определенный порядок работы с конфиденциальной информацией и доступа к ней, включающий в себя комплекс административных, правовых, организационных, инженерно-технических, финансовых, социально-психологических и иных мер, основывающихся на государственных правовых нормах и на организационно-распорядительных положениях руководителей субъекта предпринимательской деятельности. Вопросы, связанные с коммерческой тайной достаточно подробно рассмотрены в п.1.3. настоящей работы.

Как было отмечено ранее, в настоящее время отсутствует какая-либо универсальная методика, позволяющая четко относить ту или иную информацию к категории коммерческой тайны. Законопроектом «О коммерческой тайне» права по отнесению информации к категории коммерческой тайны предоставлены руководителям хозяйствующих субъектов.

Поэтому при разработке политики информационной безопасности руководителям субъектов инновационной деятельности целесообразно определить функции по защите коммерческой тайны субъекта хозяйствования:

- Выработать критерии выделения ценной информации, подлежащей защите.
- Определить объекты интеллектуальной собственности, подлежащие охране.
- Выбрать методы защиты (патентование, авторское право, непосредственно защита и т.п.).
- Разработать для последующего утверждения Перечень сведений, составляющих промышленные секреты.
- Установить правила допуска и разработать разрешительную систему доступа к сведениям, составляющим промышленные секреты.

Для того, чтобы разработать эффективную политику безопасности, информация, хранимая или обрабатываемая в организации, должна быть

классифицирована, по нашему мнению, прежде всего в соответствии с ее критичностью к потере конфиденциальности. На основе этой классификации разрабатывается политика для разрешения (или запрещения) доступа к информационным ресурсам.

В развитии п.1.3. настоящей работы, заметим, что наиболее рационально разбить информационные ресурсы на 4 класса безопасности, каждый из которых имеет свои требования по обеспечению защиты - критичная информация, коммерческая тайна, персональная информация и для внутреннего пользования. Эта система классификации должна использоваться во всей организации. Лица, ответственные за информационные ценности, отвечают за назначенные им классы информационных ресурсов, и этот процесс должен контролироваться руководством предприятия. Классы определяются следующим образом:

- Критичная информация:

Этот класс применяется к информации, требующей специальных мер безопасности для обеспечения гарантий ее целостности, чтобы защитить ее от модификации или удаления. Эта информация требует более высоких гарантий, чем обычно, в отношении ее точности и полноты. Примерами информации этого класса может служить информация о финансовых операциях или распоряжения руководства.

- промышленные секреты:

Этот класс применяется к наиболее критической промышленной и научной информации, которая предназначена для использования только внутри организации, если только ее разглашение не требуется различными законодательными актами. Ее несанкционированное разглашение может нанести серьезный вред организации, ее акционерам, деловым партнерам и клиентам.

- Персональная информация:

Этот класс применяется к информации личного характера, использование которой разрешено только внутри организации. Ее раскрытие может нанести серьезный вред организации и ее персоналу.

- Для внутреннего пользования:

Этот класс применяется ко всей остальной информации, которая не попадает ни в один из указанных выше классов. Хотя ее раскрытие нарушает политику, оно не может нанести какого-либо вреда организации, ее служащим или клиентам.

Второй вопрос «От кого (от чего) защищать?» тесно связан с понятием «угроза». Методики анализа риска и сценарного анализа поведения системы ИБ, учитывающие модели нарушителей (приложение 8), предложенные во 2-ой главе работы, позволяют полно ответить на этот вопрос. Считаем необходимым отметить, что наиболее неуправляемым элементом в системе защиты информации является персонал. Правильно разработанная кадровая политика и организация управления персоналом позволяют снизить риски этого фактора. Хотя при обсуждении вопросов информационной безопасности часто основное внимание уделяется внешним злоумышленникам, в действительности, как

показывает практика, подавляющее большинство инцидентов связано с ошибками или преднамеренными действиями служащих компании. Поэтому грамотно разработанная политика безопасности должна включать программу защиты от персонала, которая охватывает угрозы от различных типов нарушителей, включая служащих, деловых партнеров, поставщиков и подрядчиков. Проверки во время работы и тщательный мониторинг ее выполнения являются важными компонентами защиты от персонала.

Проведение кадровой политики, нацеленной на решение задачи обеспечения информационной безопасности, на всех уровнях управления коммерческим предприятием основывается на трех основных положениях:

- Безопасность при выборе персонала и работе с ним.

Это положение предполагает включение задач по обеспечению информационной безопасности в должностные обязанности всех сотрудников, строгую проверку кандидатов (проверку рекомендаций, данных резюме, идентификацию личности, подтверждение ученых степеней и образования), ознакомление и подписание соглашения о конфиденциальности.

- Подготовка и переподготовка пользователей и специалистов по защите информации.

Это положение подразумевает наличие системы повышения уровня технической грамотности и информированности пользователей в области информационной безопасности, а также переподготовку специалистов по защите информации. Для этого необходимо регулярное проведение тренингов для персонала и контроль готовности новых сотрудников по применению правил информационной защиты, а также периодическая переподготовка специалистов подразделений защиты информации.

- Реагирование на нарушения информационной безопасности.

По этому положению для организации своевременного реагирования на нарушения информационной безопасности на субъекте хозяйственной деятельности необходимо создать систему мониторинга событий информационной безопасности, которая должна включать средства системного мониторинга для автоматизированных участков обработки информации, а также регламент представления отчетов об инцидентах в области информационной безопасности для всех сотрудников предприятия и другую информацию о состоянии системы информационной защиты субъектов предпринимательской деятельности.

С третьим вопросом «как защищать?» связано понятие «система информационной защиты», как комплекса мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектов защиты.

Среди основных видов средств защиты различают нормативно-правовые, морально-этические, организационные и программно-технические.

Схематично политику безопасности инновационного предприятия можно представить, как (рис.7).

Рис.7. Политика информационной безопасности инновационного предприятия.

Разработка и внедрение политики информационной безопасности требует серьезных инвестиций – денежных, временных, человеческих ресурсов, но эффективно построенная политика окупает затраты и приносит фирме неоспоримые преимущества.

В большинстве стран и в том числе в России принято, что всю ответственность за защиту информационных активов хозяйствующих субъектов несет руководство. Так как руководители субъектов инновационной деятельности, как правило, не являются специалистами в области защиты информации, их попытки вмешиваться в техническую и организационную

сторону безопасности могут приводить к нежелательным последствиям. Если же в инновационной организации разработана политика информационной безопасности, в которой четко прописаны обязанности и уровень доступа самых разных сотрудников, то руководитель может легко контролировать выполнение этих правил. Вовлечение руководства хозяйствующего субъекта в дело информационной безопасности приносит огромную вспомогательную выгоду – оно значительно увеличивает приоритет информационной безопасности, что положительно отражается на общем уровне безопасности субъекта инновационной деятельности.

Поскольку политика отражает философию и стратегию управления, она является четким и бесспорным доказательством намерений инновационной организации относительно информационной безопасности. Это положительно сказывается на работе с клиентами и партнерами, а особенно на привлечение дополнительных инвестиций в предпринимательский бизнес. Все большее число российских, а тем более, иностранных компаний требуют доказательства достаточного уровня надежности и безопасности, особенно информационной, своих инвестиций и ресурсов.

Как уже отмечалось, политика информационной безопасности - это совершенный стандарт, которым может быть измерена целесообразность и окупаемость затрат на защиту ресурсов. Руководителю организации достаточно сравнить предлагаемые выгоды с данными, прописанными в политике информационной безопасности, чтобы определить эффективность расходования средств из бюджета компании.

Если политика правильно сформулирована и связана с трудовыми контрактами служащих, то любые нарушения установленного режима информационной безопасности могут быть наказаны согласно ранее оговоренным пунктам, подписанными служащими. Даже просто наличие подобного документа на хозяйствующем субъекте значительно улучшает информационную безопасность и улучшает производительность труда персонала. Хорошо осуществленная политика помогает гарантировать выполнение инструкций, путем создания единой директивы и ясного назначения обязанностей, а также описания ответственности за неисполнение обязанностей и негативные последствия.

При надлежащем обучении персонала, должном выполнении им своих обязанностей и используемых современных технологиях «человеческий фактор» фактически исключается из списка проблем и становится хорошей позитивной составляющей безопасности. Эффективно разработанная политика информационной безопасности может служить также эталоном, по которому возможно измерение степени компетенции, успешного выполнения своей работы и рабочей дисциплины любыми ответственными сотрудниками организации. Фактически, политика должна заранее вводить высокие стандарты информационной безопасности и затем отслеживать, чтобы весь персонал фирмы подтянул свои знания и навыки к этим стандартам и полностью нес ответственность за информационную безопасность хозяйствующего субъекта и последствий от своих противоправных действий.

Нанесение вреда информационной безопасности фирмы «по незнанию» при имеющейся политике информационной безопасности исключается.

Эффективность политики пропорциональна поддержке, которую она получает от различных структур организации и конкретных сотрудников. Таким образом, критически важным условием для успеха в области защиты информационных ресурсов фирмы становится создание в организации атмосферы, благоприятной для поддержания высокого приоритета информационной безопасности. Любая политика приходит к персоналу фирмы «сверху». Сначала руководство организации определяет какой-то вариант политики, после чего происходит принятие политики руководителями среднего и низшего звена, а затем рядовыми сотрудниками. В ходе принятия политики безопасности возможно внесение в нее согласованных с руководством корректив, а иногда, фундаментальное изменение в структуре организации и перераспределение полномочий.

Как правило, чем крупнее организация, тем более масштабные изменения в существующих правилах и порядках ей предстоят в связи с принятием политики информационной безопасности. Но, в любом случае, привитие культуры информационной безопасности позитивно отражается на безопасности субъекта инновационной деятельности в целом.

3.2. Разработка мер реализации политики информационной безопасности субъекта инновационной деятельности путем создания службы защиты информации

Отдельный раздел закона "Об информации, информатизации и защите информации", посвященный организации информационной защиты, определяет необходимый комплекс мероприятий [152]:

- установление особого режима конфиденциальности;
- ограничение доступа к конфиденциальной информации;
- использование организационных мер и технических средств защиты информации;
- осуществление контроля за соблюдением установленного режима конфиденциальности.

Конкретное содержание указанных мероприятий для каждого отдельно взятого хозяйствующего субъекта может быть различным по масштабам и формам. Это зависит в первую очередь от производственных, финансовых и иных возможностей предприятия, от объемов конфиденциальной информации и степени ее значимости. Существенным является то, что весь перечень указанных мероприятий обязательно должен планироваться и использоваться с учетом особенностей функционирования информационной системы предприятия.

Необходимые мероприятия по защите информации достаточно подробно освещены в предыдущем пункте данной главы. Считаем важным отметить, что традиционно для организации доступа к конфиденциальной информации

использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями (приложение 9), приказами, договорами (приложения 1, 11) и другими нормативными документами. Однако с развитием компьютерных систем эти меры перестали обеспечивать необходимую безопасность информации. Появились и в настоящее время широко применяются специализированные программные и программно-аппаратные средства защиты информации, которые позволяют максимально автоматизировать процедуры доступа к информации и обеспечить при этом требуемую степень ее защиты.

Осуществление контроля за соблюдением установленного режима конфиденциальности предусматривает проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации. Как правило, контроль осуществляется в виде плановых и внеплановых проверок. По результатам проверок специалистами по защите информации проводится необходимый анализ с составлением отчета, который включает:

- вывод о соответствии проводимых на предприятии мероприятий установленным требованиям;
- оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

Обеспечение и реализация перечисленных выше мероприятий требует создания на инновационном предприятии соответствующих органов защиты информации. Эффективность защиты информации на субъекте инновационной деятельности во многом будет определяться тем, насколько правильно выбрана структура органа защиты информации и квалифицированы его сотрудники. Как правило, служба защиты информации представляет собой самостоятельное подразделение.

Созданием службы защиты информации на инновационном предприятии завершается построение системы информационной безопасности, под которой понимается совокупность органов защиты информации, используемые ими средства защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации. В состав пакета организационных-распорядительных документов хозяйствующего субъекта могут входить различные документы, регулирующие вопросы обеспечения информационной безопасности, примерный их перечень приведен в приложении 11.

Основными функциями службы защиты информации инновационной фирмы являются следующие:

- организация и осуществление совместно с подразделениями фирмы защиты конфиденциальной информации;
- проверка сведений о попытках шантажа, провокаций и иных акций в отношении персонала, преследующих цель получения конфиденциальной информации о деятельности фирмы;

- организация сбора, накопления, автоматизированного учета и анализа информации по вопросам безопасности;
- проведение проверок в подразделениях фирмы и оказание им практической помощи по вопросам информационной безопасности их деятельности;
- разработка и внедрение положения о промышленных секретах;
- проверка правил ведения закрытого делопроизводства;
- проверка работников на предмет соблюдения правил обеспечения экономической, информационной и физической безопасности;
- оказание содействия отделу кадров по работе с персоналом в вопросах подбора, расстановки, служебного перемещения и обучения персонала;
- сбор, обработка, хранение, анализ информации о контрагентах с целью предотвращения сделок с недобросовестными партнерами;
- выполнение поручений руководства фирмы, входящих в компетенцию службы;
- взаимодействие с правоохранительными органами, проведение мероприятий по выявлению и предупреждению различного рода финансово-хозяйственных правонарушений;
- проведение служебных расследований по фактам разглашения конфиденциальной информации, потери служебных документов работниками фирмы и действий угрожающих экономической безопасности фирмы.

Организация, задачи и функции службы защиты информации коммерческой структуры закрепляются в Положении о службе защиты информации, пример которого приводится в приложении 12.

Правовой базой для создания службы безопасности является Закон РФ от 11 марта 1992 г. “О частной детективной и охранной деятельности в Российской Федерации” № 2487-1, которым предусматривается (ст. 14), что предприятия, расположенные на территории Российской Федерации, независимо от их организационно - правовых форм, вправе учреждать обособленные подразделения - службы безопасности, для осуществления деятельности по защите безопасности собственных экономических интересов.

Создание собственной службы информационной защиты представляет на практике определенную трудность, поскольку каждый субъект предпринимательства сугубо индивидуален, поскольку специфична его деятельность. Однако, можно выделить ряд этапов, рекомендуемых предпринимателям при создании службы безопасности:

1.Принятие решения о необходимости создания службы защиты информации.

Вопрос о создании службы защиты информации в идеале должен возникать в момент принятия решения об организации хозяйствующего субъекта, в зависимости от выбираемого вида деятельности, размера годового оборота и прибыли, использования секретов производства, количества работников и т.п. Учредители должны заранее предусмотреть необходимость

создания службы защиты информации и определить ответственное лицо, которое будет непосредственно заниматься организацией этой службы. Если необходимость создания службы защиты информации созрела в процессе функционирования фирмы, то, как правило, такая служба создается в процессе разработки политики информационной безопасности хозяйствующего субъекта.

2. Определение общих задач службы защиты информации.

В задачи службы защиты информации входит: предупреждение угроз, реагирование на возникшие угрозы и определение конкретных объектов защиты (персонал, конфиденциальная информация, компьютерные системы, здания и помещения).

3. Разработка положения о службе защиты информации.

В нем определяется структура, и утверждается штат службы. Наличие соответствующей законодательной базы позволяет создать легальную службу безопасности (приложение 11).

4. Набор кадров в службу информационной безопасности.

Работниками службы информационной безопасности могут быть люди, специально и постоянно занимающиеся данной деятельностью как основной и привлеченные специалисты (например, главный бухгалтер, юрист и пр.).

При подборе постоянных работников в качестве важнейшего требования выступает профессиональная подготовка. В связи с этим предпочтение следует отдавать высококвалифицированным специалистам в области безопасности и бывшим работникам правоохранительных органов (МВД, ФСБ, прокуратуры, налоговой полиции) с соответствующим опытом работы и морально-деловым качествами для данной деятельности.

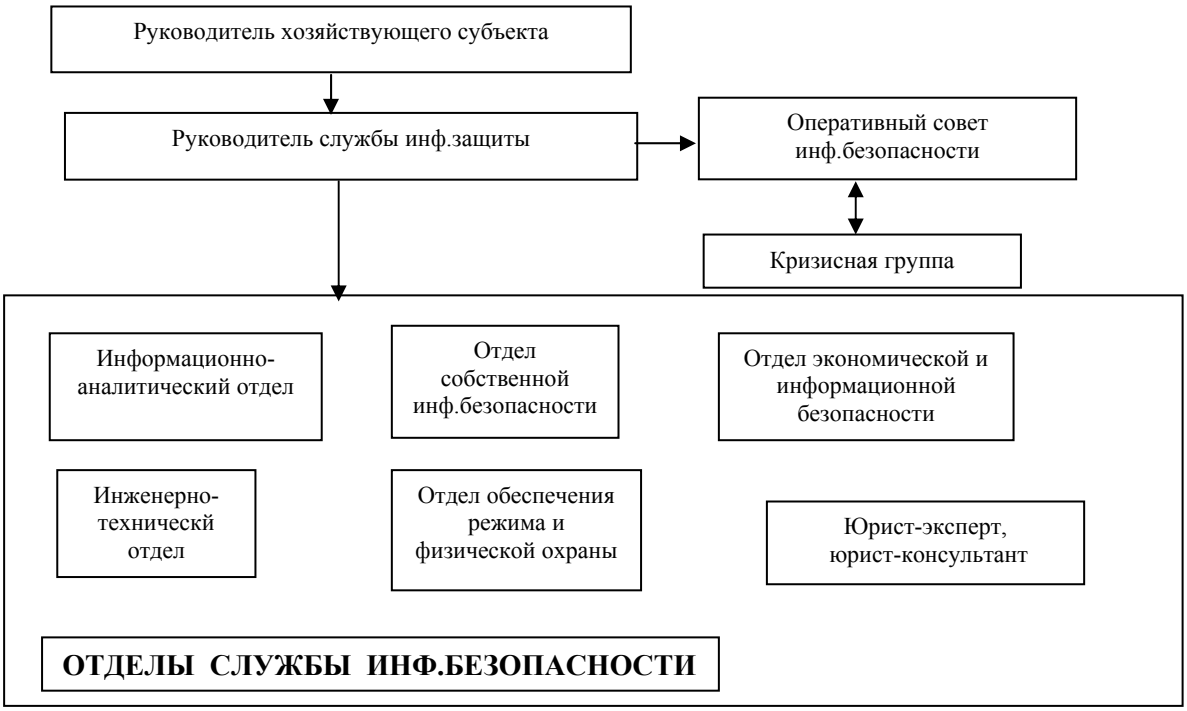

Рис. 8. Примерная структура службы защиты информации инновационного предприятия.

5.Непосредственная организация и функционирование службы защиты информации.

В процессе функционирования службы значительную роль играет умелая расстановка кадров, распределение прав, полномочий и степени ответственности, что позволяет обеспечить эффективную работу подразделения.

Примерная рекомендуемая нами структура службы защиты информации хозяйствующего субъекта приведена на рис.8.

Особое положение в структуре службы защиты информации, по нашему мнению, занимает кризисная группа, осуществляющая свою деятельность совместно с оперативным советом по информационной безопасности. Предварительно следует заметить, что фирма, а значит и служба защиты информации, могут работать в двух режимах – обычном и чрезвычайном. При обычном режиме не возникает серьезных угроз информационной безопасности фирмы, идет профилактическая работа по их предупреждению и деятельность всех подразделений проходит в повседневном ритме. Возникающие проблемы и угрозы носят локальный характер и преодолеваются текущей работой подразделений фирмы, в том числе службой защиты информации. При чрезвычайном режиме возникают неожиданные угрозы с высокой или значительной тяжестью последствий. В этом случае руководитель службы защиты информации собирает группу чрезвычайных ситуаций (кризисную группу), включающую наиболее квалифицированных в данной проблеме

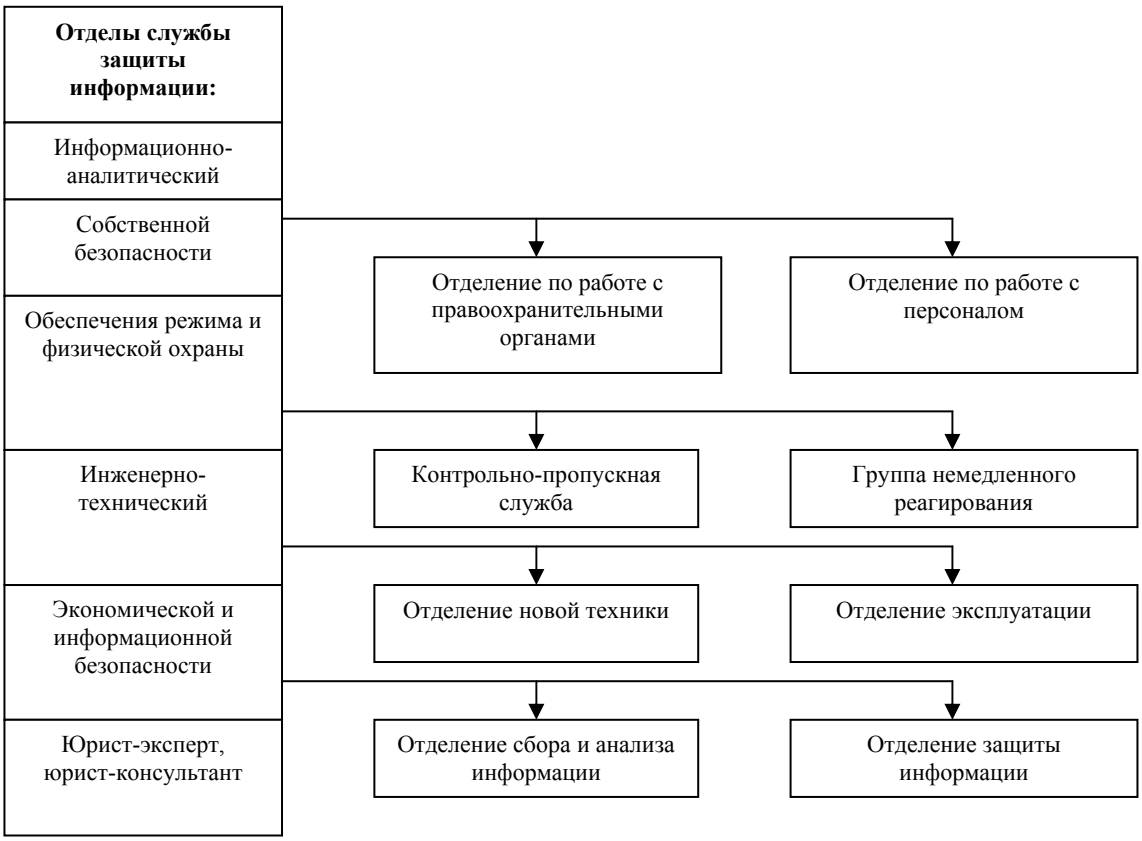

Рис. 9. Примерная схема организации отделов службы защиты информации.

специалистов фирмы, для ее решения. Эта группа работает не постоянно, а лишь по мере необходимости.

Отделы службы защиты информации часто состоят из отделений, отвечающих за конкретные направления в рамках работы данных отделов. Предлагаем примерную схему организации отделов службы:

Основные функции отделов службы безопасности:

1. Информационно-аналитический отдел:

оптимизирует деятельность службы защиты информации, минимизирует риски и максимизирует прибыли. Участвует в разработке политики информационной безопасности организации и проектировании интегрированной системы безопасности. Должен работать непрерывно, отслеживая изменение параметров системы. Разрабатывает оперативно-тактические планы.

2. Отдел собственной безопасности:

обеспечивает контроль персонала, проверку деятельности персонала по обеспечению безопасности, усилению исполнительской дисциплины, взаимодействие с правоохранительными органами. Подсистема функционирует на основе принципов объективности, систематичности, своевременности, конкретности, целенаправленности. Используемые методы: наблюдение, обследование, эксперимент. По результатам контрольно-проверочных мероприятий разрабатываются конкретные предложения по устранению имеющихся недостатков и оказанию практической помощи исполнителям в совершенствовании работы.

3. Отдел обеспечения режима и физической охраны:

обеспечивает сохранность материальных ценностей, физических носителей информации и персонала от потенциально возможных угроз.

4. Инженерно-технический отдел:

на основе разработанной политики информационной безопасности обеспечивает оптимальное распределение технических средств по всей структуре службы защиты информации. Осуществляет контроль работы, своевременное обновление и внедрение парка новых технических средств. За счет этого достигается минимизация людских и иных ресурсов в процессе обеспечения информационной безопасности, а также обеспечивается максимальная надежность охраны, минимальные затраты на эксплуатацию.

5. Отдел экономической и информационной безопасности:

обеспечивает безопасность экономической деятельности организации и защиту ее коммерческой тайны. Осуществляет получение дополнительной информации об экономическом пространстве и его изменении законными путями. Обеспечивает защиту от промышленного шпионажа, недобросовестной конкуренции, разведывательных мероприятий других организаций. Осуществляет взаимодействие со средствами массовой информации.

6. Юрист-эксперт, юрист-консультант:

осуществляет детальный анализ всех документов, подлежащих утверждению руководителями организации. Контроль документооборота, экспертиза договоров и своевременный учет изменения законодательства, разработка

правовых мер по предотвращению негативных для организации явлений (ликвидации организации, штрафных санкций, юридических исков и т.п.).

7. Оперативный совет безопасности:

является консультационным органом службы защиты информации и служит для разрешения спорных и сложных вопросов в осуществлении деятельности службы. В этот совет входят руководитель организации и ведущие специалисты из всех подразделений службы защиты информации, председателем является, как правило, руководитель организации.

8. Кризисная группа:

оказывает противодействие внезапно возникающим критическим (кризисным) ситуациям, то есть оценке обстановки, принятию неотложных мер по информационной безопасности, управлению деятельностью фирмы в экстренных условиях, обеспечению оперативного взаимодействия с органами правопорядка. Она создается из числа ключевых фигур организации: руководителя, начальников подразделений, филиалов, служб, юриста, главного бухгалтера и др. В каждом конкретном случае в состав кризисной группы могут включаться те или иные специалисты. Рабочие заседания группы должны проходить в условиях предельной конфиденциальности.

Особое внимание следует уделять постоянному взаимодействию службы защиты информации с правоохранительными органами.

Взаимодействие службы защиты информации и правоохранительных органов может осуществляться по следующим направлениям:

- Кадры – проверка правоохранительными органами кандидатов на работу, подготовка с помощью правоохранительных органов работников служб информационной безопасности.
- Информация – обмен взаимной информацией о способах совершения противоправных действий, потенциально опасных лицах и пр.
- Организационное взаимодействие – создание системы совместного противодействия незаконной деятельности со стороны физических и юридических лиц (организация охраны, установка сигнализации, системы быстрого оповещения правоохранительных органов).

Особо важное значение для минимизации негативных последствий возникших угроз играет своевременное и оперативное информирование сотрудниками службы защиты информации правоохранительных органов об обнаружении правонарушений, приведших к негативным последствиям для коммерческой организации и повлекшим наступление ответственности, носящей одновременно как гражданско-правовой, так и уголовный характер.

Практическая деятельность службы защиты информации должна основываться на использовании типовых схем, процедур и действий. Прежде всего следует сказать об общем алгоритме действий, на котором основана работа службы защиты информации. Он включает следующую последовательность операций (рис.10):

Рис. 10. Алгоритм действий службы защиты информации.

Система предупредительных мер включает деятельность по изучению контрагентов, анализу условий договоров, соблюдению правил работы с конфиденциальной информацией, защите компьютерных систем и т.д. Эта деятельность осуществляется регулярно и непрерывно. Она обеспечивает защиту информационной безопасности на основе постоянно действующей системы организационных мероприятий.

В заключении необходимо отметить:

При построении политики информационной безопасности руководитель хозяйствующего субъекта и начальник службы защиты информации должны очень тщательно анализировать полный набор угроз, глубокое знание и своевременное выявление которых позволит службе защиты информации превентивно их блокировать.

Накопленный в мире опыт в области безопасности показывает, что:

- Анализ угроз и разработка политики информационной безопасности не должны быть одноразовыми актами. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы информационной безопасности, непрерывном управлении ей, контроле, выявлении ее слабых мест и ликвидации недостатков;
- Информационная безопасность может быть обеспечена лишь при комплексном использовании всего арсенала сил и средств во всех структурных элементах системы, то есть использовании комплексной системы информационной безопасности;
- Никакая комплексная система информационной безопасности не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала организации и пользователей и соблюдения ими всех установленных правил, направленных на обеспечение информационной безопасности.

3.3. Определение роли мониторинга системы информационной безопасности и его значение в формировании политики информационной безопасности инновационных организациях

Для обеспечения высокой конкурентоспособности инновационной деятельности путем поддержания информационной безопасности и противодействия внутренним и внешним угрозам коммерческим интересам фирмы важнейшее значение принадлежит мониторингу правильного функционирования системы защиты информационной безопасности хозяйствующего субъекта.

Мониторинг системы информационной безопасности – это деятельность, направленная на проверку, контроль, анализ и оценку текущего положения и прогноз в области информационной безопасности субъекта предпринимательской деятельности.

Мониторинг системы информационной безопасности понимается сегодня достаточно широко. За этим названием скрываются, по крайней мере, три различных группы работ:

К первой группе относятся так называемые «тестовые взломы» систем информационной безопасности предприятия. Но, как показывает практика, этот подход является мало эффективным. Причина малой эффективности «тестовых взломов» с точки зрения получения сведений об информационной безопасности ресурсов предприятия скрывается в самой постановке задачи. Как правило, основной задачей является обнаружение одной-двух уязвимостей и их максимальная эксплуатация для доступа в систему. Если тест оказался успешным, то, предотвратив потенциальное развитие возможных сценариев тестовой атаки, работу необходимо начинать сначала и искать следующие. Неуспех атаки может означать в равной мере, как защищенность системы, так и недостаточность тестов.

Вторая группа работ по проведению мониторинга информационной безопасности хозяйствующего субъекта - экспресс-обследование. В рамках этой, обычно непродолжительной, работы оценивается общее состояние механизмов безопасности информационных ресурсов на основе стандартизованных проверок. Экспресс-обследование обычно проводится в случае, когда необходимо проконтролировать функционирование системы информационной безопасности фирмы и определить приоритетные направления, позволяющие обеспечить минимальный уровень защиты информационных ресурсов. Основу для него составляют списки контрольных вопросов, заполняемые как в результате интервьюирования персонала, так и в результате работы автоматизированных сканеров защищенности.

Третья группа работ по проведению мониторинга информационной системы хозяйствующего субъекта является самой трудоемкой, проводится полное обследование защищенности информационной системы данного субъекта. Такое обследование предполагает анализ организационной структуры

предприятия в приложении к информационным ресурсам, правил доступа сотрудников к тем или иным информационным ресурсам.

Затем выполняется анализ самих информационных ресурсов. Картина дополняется встроенными механизмами безопасности, что в сочетании с оценками потерь в случае нарушения информационной безопасности дает основания для ранжирования рисков, существующих в информационной системе, и выработки адекватных контрмер. Успешное проведение полного обследования и анализа рисков определяет, насколько принятые меры будут, с одной стороны, экономически оправданы, с другой — адекватны угрозам. Применение методологии сценарного анализа позволяет эффективно справиться с этой задачей.

Мониторинг системы информационной безопасности следует рассматривать как инструмент в формировании политики информационной безопасности предприятия.

Политику информационной безопасности можно представить как совокупность следующих этапов, среди которых мониторинг играет одну из ключевых ролей (рис. 11.):

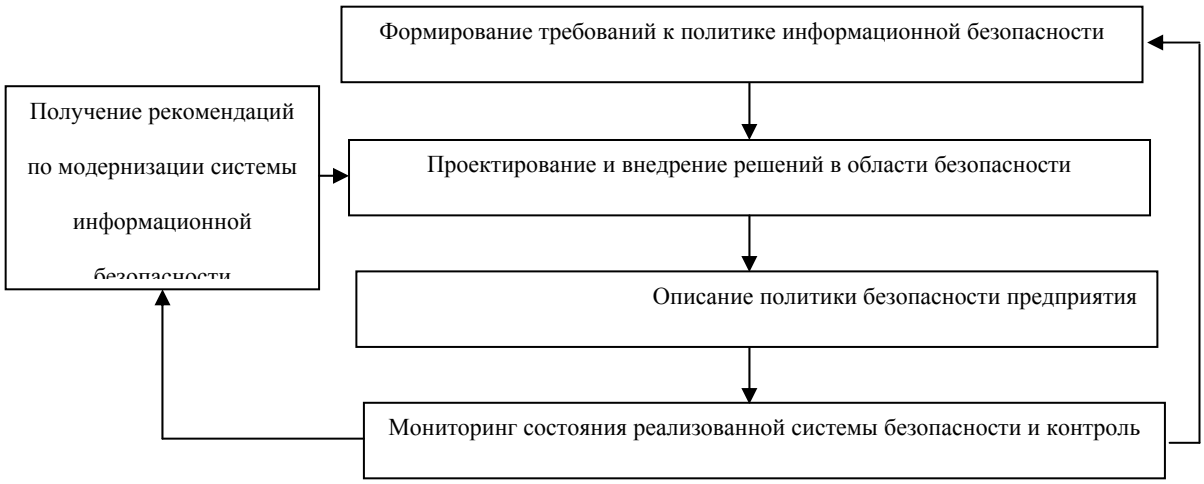

Рис. 11. Роль и место мониторинга в формировании политики безопасности инновационной предприятия.

На этапе формирования требований к политике информационной безопасности определяются требования защищенности имеющейся информационной системы хозяйствующего субъекта, это подробно рассмотрено в п.3.1.

Следующий этап – непосредственно проектирование и построение системы информационной безопасности коммерческого предприятия, включающее в себя комплекс организационных мер и технических средств защиты информации.

Назначение системы информационной безопасности субъекта инновационной деятельности реализуется в ее политике информационной безопасности.

Мониторинг состояния реализованной системы защиты информации и контроль соблюдения политики информационной безопасности позволяют своевременно выявить существующие бреши в безопасности хозяйствующего субъекта и объективно оценить соответствие параметров, характеризующих режим безопасности, необходимому уровню.

Под мониторингом подразумевается оценка текущего состояния безопасности на соответствие основно-правовым актам, методологическим документам по ИБ (приложение 1) и предъявленным при выработке политики информационной безопасности требованиям.

В процессе проведения проверки анализируются и оцениваются следующие положения:

1. Организационная инфраструктура информационной безопасности на местах (распределение обязанностей сотрудников по обеспечению безопасности);

2. Документированная политика безопасности предприятия, и в частности:

- подход к оцениванию и управлению рисками в рамках всей организации;
- обоснование выбора средств защиты;
- процедура принятия уровня остаточного риска;
- результаты оценивания рисков по информационной системе предприятия;
- контрмеры для противодействия выявленным рискам;
- эффективность использования контрмер и результаты их тестирования и т.д.

В процессе проверки на соответствие требованиям безопасности могут быть получены следующие ответы:

- да, это требование полностью выполняется;
- частично, некоторые положения выполняются, но этого недостаточно для положительного ответа;
- нет, это требование не выполняется, либо к данной системе оно не применимо.

Если требование не выполняется или выполняется частично, то указывают причину (или причины) этого, относя их к одной из следующих категорий:

- это требование ранее не учитывалось, считалось несущественным;
- финансовые ограничения;
- препятствуют внешние факторы (климатические факторы и т.д.);
- временные ограничения (не все требования могут быть выполнены одновременно, впоследствии по мере возможностей постепенно будут выполнены);
- прочее.

На основе ответов составляется «Ведомость соответствия». Основная цель этого документа – дать аргументированное обоснование имеющих место отклонений предъявленных при выработке политики безопасности требований.

После проведенной проверки необходимо иметь четкое представление о степени серьезности обнаруженных недостатков, их категориях и способах исправления. В практике используются следующие категории несоответствия:

- Существенное несоответствие.

Не выполняется одно или несколько базовых требований, либо установлено, что используются неадекватные меры защиты конфиденциальности, целостности или доступности критически важной информации.

- Несущественное несоответствие.

Не выполняются некоторые второстепенные требования, что влечет за собой некоторое повышение рисков или снижение эффективности защитных мер.

Каждое несоответствие имеет ссылку на соответствующее требование по обеспечению информационной безопасности.

В итоге работы необходимо проанализировать все существенные аспекты информационной безопасности с учетом величины проверяемой организации и специфики ее деятельности, учесть ценность информации, подлежащей защите. Как следствие, опыт и компетентность специалистов, проводящих мониторинг, являются весьма существенными факторами, оказывающими влияние на итоговый результат.

В результате проведения мониторинга создается список выявленных несоответствий требованиям ИБ или замечаний, а также рекомендации по их исправлению.

Для проведения мониторинга системы информационной безопасности создается специальная комиссия. Руководитель фирмы совместно с руководителем службы безопасности определяет ее членов из числа наиболее надежных и квалифицированных работников фирмы. В необходимых случаях могут привлекаться и внешние специалисты. Но тенденции развития этого направления таковы, что руководители коммерческих фирм все чаще склоняются к созданию службы внутрифирменного мониторинга, поскольку гораздо дешевле предотвратить правонарушения собственными силами, чем потом бороться с их последствиями.

На основе результатов проведенного мониторинга системы информационной безопасности хозяйствующего субъекта разрабатывается проект, назначение которого состоит в модернизации старых и внедрении новых схем защищенного взаимодействия в рамках информационной системы хозяйствующего субъекта, что находит свое отражение в новом доработанном варианте политики информационной безопасности предприятия. Регулярный мониторинг системы информационной безопасности является одним из обязательных условий сохранения адекватного уровня информационной безопасности фирмы.

Поэтому, основываясь на вышесказанном и подводя итог 3-ей главе, можно сделать следующие выводы:

- В основе разработки комплексной и эффективной системы обеспечения экономической безопасности инновационного предпринимательства в аспекте защиты его коммерческих и технологических интересов и в целях поддержания его конкурентоспособности на внутреннем и мировом рынках в должна лежать определенная политика информационной безопасности, которая включает описание цели комплексной системы защиты, ее задачи, принципы деятельности, философию безопасности, стратегию и тактику, а также объект и субъект защиты.
- Наличие эффективно разработанной политики безопасности является четким и бесспорным доказательством намерений субъекта хозяйственной деятельности относительно информационной защиты, что положительно сказывается на его положении на конкурентном рынке, работе с партнерами, на повышении производительности труда персонала, на привитии культуры информационной безопасности на хозяйствующем субъекте и на привлечении инвестиций в инновационный бизнес.
- Политика информационной безопасности предполагает разработку специальных мер организационного и технического характера, среди которых особое место занимает создание службы собственной информационной безопасности.
- Разработка политики информационной безопасности субъекта инновационной деятельности начинается с формирования требований к безопасности информационных ресурсов предприятия. От качественного проведения этого этапа зависит уровень всех дальнейших проектных решений по защите информационной среды предприятия.
- Мониторинг состояния реализованной системы информационной безопасности является важнейшим инструментом в формировании политики информационной безопасности хозяйствующего субъекта, что позволяет оценить текущее состояние безопасности на соответствие предъявленным требованиям ИБ, выявить существующие бреши в защищенности предприятия и дать рекомендации по их исправлению.
- На основе результатов мониторинга разрабатываются и внедряются новые решения в рамках информационной системы хозяйствующего субъекта. Это находит свое отражение в доработанном новом варианте политики безопасности хозяйствующего субъекта.
- Так как процесс совершенствования политики информационной безопасности хозяйствующего субъекта имеет постоянный циклический характер, поэтому мониторинг системы безопасности является одним из обязательных условий сохранения адекватного уровня информационной безопасности коммерческой фирмы.

ЗАКЛЮЧЕНИЕ

Стремительное развитие информационных технологий на современном этапе, признание конкуренции как главного фактора, обеспечивающего преимущество на рынке отдельных фирм, активизация промышленной разведки привели в настоящее к необходимости пересмотра традиционных подходов к обеспечению сохранения конфиденциальной информации и промышленных секретов хозяйствующих субъектов. В поддержании высокой конкурентоспособности инновационной деятельности особое место принадлежит проблеме формирования эффективной системы информационной безопасности хозяйствующих субъектов.

Изложенные в монографии теоретические, организационные и прикладные проблемы построения и функционирования системы ИБ субъекта инновационной деятельности позволили подробно рассмотреть наиболее существенные вопросы, относящиеся к построению эффективной политики информационной безопасности данных субъектов. Данный факт особенно существенен и актуален в настоящее время, так как без обеспечения стройной и целенаправленной организации процесса противодействия недобросовестной конкуренции, различного рода угрозам конфиденциальной информации невозможно создать условия для безопасного и устойчивого развития и функционирования инновационных структур на внутреннем и мировом конкурентных рынках.

В монографии был обобщен и систематизирован круг проблем, относящихся к обеспечению безопасности информационной среды инновационной деятельности. Проведенный анализ показал, что обеспечение защиты информационных ресурсов хозяйствующих субъектов решается построением системы информационной безопасности данных субъектов. Причем только комплексный подход к обеспечению информационной безопасности, предполагающий рациональное сочетание правовых, программно-технических и организационных мер, способен эффективно решить данную проблему.

На основе проведенного исследования автороми сделан вывод, что функционирование системы обеспечения информационной безопасности инновационного предпринимательства должно основываться на 4-х уровнях:

- создание политико-правовых международных условий существования субъектов инновационной деятельности в рамках государства;
- обеспечение достижимости макроэкономических целей на федеральном и региональном уровнях путем создания внутригосударственной подсистемы экономической безопасности;
- создание объектовой защиты субъектов инновационной экономики от противоправных посягательств с использованием сил и средств самих объектов защиты;

- обеспечение непосредственно информационной защиты хозяйствующих субъектов путем построения систем информационной безопасности и внедрения политики безопасности на данных субъектах.

Авторами были проанализированы понятия конфиденциальной информации, ее основных категорий и промышленных секретов субъектов инновационной деятельности. В рамках предложенной классификации выделены составляющие промышленных секретов по функционально-целевому признаку, детально исследованы сущность и признаки угроз конфиденциальной информации, что позволило сделать вывод о необходимости построения политики информационной безопасности субъекта инновационной деятельности на основе комплексного подхода, учитывающего многообразие потенциальных угроз информации, назначение объекта защиты, его размеров, условий размещения и характера деятельности.

В монографической работе авторы делают вывод, что в основе разработки комплексной и эффективной системы обеспечения экономической безопасности инновационного предпринимательства в аспекте защиты его коммерческих интересов и, таким образом, обеспечения его конкурентоспособности, должна лежать определенная политика информационной безопасности, которая включает описание философии безопасности, цели комплексной защиты, ее задачи, принципы деятельности, а также стратегию и тактику защиты.

Авторами была подробно исследована модель построения политики информационной безопасности хозяйствующих субъектов, принципиально важным моментом которой является формирование требований к безопасности информационных ресурсов, подробно рассмотрены и классифицированы основные угрозы информационной безопасности деятельности данных субъектов.

В работе предложена и апробирована модель организации отделов службы безопасности, созданием которой и завершается построение системы защиты информации субъекта инновационной предпринимательской деятельности. Выделены ряд этапов, рекомендуемых при создании службы безопасности, описаны функции отдельных подразделений и обоснована необходимость создания кризисной группы для принятия решений при чрезвычайных обстоятельствах, приведен алгоритм действий службы безопасности.

На основе проведенного исследования выявлены роль и место мониторинга системы защиты ИБ в формировании политики информационной безопасности инновационной структуры, проведение которого носит постоянный циклический характер и позволяет оценить текущее состояние безопасности на соответствие предъявленным требованиям, выявить существующие бреши в защищенности хозяйствующего субъекта и дать рекомендации по их исправлению.

СПИСОК ЛИТЕРАТУРЫ

1. Гражданский кодекс РФ.- ЭКМОС, 2003. - 272с.
2. Кодекс РФ об административных правонарушениях (с постатейными материалами). – М.: Юридическая литература, 2002. – 1008с.
3. Уголовный кодекс РФ. – Вече, 2003. - 160с.
4. О частной детективной и охранной деятельности в Российской Федерации. – Закон РФ №2487-1 от 11.03.92.
5. О правовой охране программ для электронных вычислительных машин и баз данных. – Закон РФ №3523-1 от 23.09.92.
6. О сертификации продукции и услуг. – Закон РФ №5151-1 от 10.06.93.
7. Об информации, информатизации и защите информации. – Закон РФ №24-ФЗ от 20.02.95.
8. Об участии в международном информационном обмене. – Закон РФ №85-ФЗ от 04.07.96.
9. Доктрина информационной безопасности Российской Федерации. - № Пр.-1895. Утверждена Президентом Российской Федерации 9.09.2000.
10. О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации. - Указ Президента Российской Федерации № 334 от 3.04.95.
11. Перечень сведений конфиденциального характера. - Указ Президента Российской Федерации № 188 от 06.03.97.
12. О передаче сведений, которые не могут составлять коммерческую тайну. - Постановление правительства Российской Федерации № 35 от 05.12.91.
13. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти. - Постановление Правительства Российской Федерации №1233 от 03.11.94.
14. Положение о лицензировании деятельности по технической защите конфиденциальной информации. – Постановление Правительства Российской Федерации №290 от 30.04.2002.
15. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации - Руководящий документ. - Гостехкомиссия России - Москва , 1992.
16. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники - Руководящий документ. - Гостехкомиссия России - Москва, 1992.
17. Защита от несанкционированного доступа к информации. Термины и определения. - Руководящий документ. – Гостехкомиссия России - Москва, 1992.

18. Концепция защиты СВТ и АС от НСД к информации. - Руководящий документ. - Гостехкомиссия России - Москва , 1992.
19. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. - Руководящий документ. - Гостехкомиссия России - Москва, 1992.
20. Специальными требованиями и рекомендациями по технической защите конфиденциальной информации» (СТР-К). - Решение Коллегии Гостехкомиссии России №7.2 от 02.03.01.
21. Азоев Г.Л. Конкуренция: анализ, стратегия и практика. – М.: Центр экономики и маркетинга, 1996. - с.56-69.
22. Алаухов С.Ф., Коцеруба В.Я. Вопросы создания систем физической защиты для крупных промышленных объектов // Системы безопасности. 2001. - №41, - с.93.
23. Андреевский Н.А. Подход к построению математической модели системы защиты информации в компьютерной системе // Безопасность информационных технологий №2, 1995. - с.16-17.
24. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. – М.: Мир, 1999. - 351с.
25. Алексеев А.И, Комментарий специалиста.// Частный сыск и охрана №1, 1998. - с.34-36.
26. Архипова Н.И., Кононов Д.А., Кульба В.В., Чернов И.В. Теоретические основы сценарного анализа как методологии построения систем управления безопасностью социально-экономических систем — // Проблемы регионального и муниципального управления. Материалы Международной конференции. 18 мая 2000г. — М.: РГГУ. 2000. с.38-39.
27. Балыбердин А.Л. Основные положения закона Российской Федерации «О государственной тайне» и их влияние на систему защиты информации. // Безопасность информационных технологий №1,. 1999. - с.7-10.
28. Бачило И.Л. Методология решения правовых проблем в области информационной безопасности. // Информатика и вычислительная техника №3, 2000. - с.21-25.
29. Батурин Ю.М. Жиджитский А.М. Компьютерная преступность и компьютерная безопасность – М.: Юридическая литература, 1999 – 162с.
30. Бережье Ж. Промышленный шпионаж. – М., 1992. - 165с.
31. Близнец И.А., Леонтьев К.Б. Роль государства в области авторского права и смежных прав // Российская юстиция. -1999. - № 11.
32. Бородина О.А. «Факторы и методы оценки экономической безопасности предприятия». Автореферат диссертации канд. экон. Наук – Донецк, 2002 - 25с.
33. Воловик Е.М. Защита данных в распределенных системах // Мир ПК. №10, 1997. - с.166-170.
34. В США принят план защиты информационных систем // Jet Info online, 2000г. - №8(87).

35. Гавриш В.А.. Практическое пособие по защите коммерческой тайны. Симферополь: Таврида, 1994. - 112с.
36. Гасанов РМ. Шпионаж и бизнес. – М., 1999. - 213с.
37. Герасименко В.А. «Основы информационной грамоты» М.: Энергоатомиздат, 1996. - 146с.
38. Герасименко В.А. Комплексная защита информации в современных системах обработки данных. // Зарубежная радиоэлектроника №2,1994 - с.35-38.
39. Горячев В.С. Информация и ее защита. // Вопросы защиты информации. №2,1994 – с.45.
40. Гранберг А.Г., Суспицын С.А. Введение в системное моделирование народного хозяйства. – Новосибирск: Наука. Сиб. отд-ние, 1988. - 304с.
41. Гузик С. Зачем проводить аудит информационных систем? // Jet Info online, № 10(89), 2000.
42. Гуров А.И. Профессиональная преступность: прошлое и современность – М.,1996. - 116с.
43. Давыдовский А.И. Методология построения безопасных процессов обработки информации. // Безопасность информационных технологий. №1, 1999. - с.63-65.
44. Данько Т.П. Управление маркетингом: Учебник. Изд. 2-е, перераб. и доп. – М.: ИНФРА-М, 2001. - 334с.
45. Долгова А.И. Преступность в России // Советская юстиция. – 1993, с.37-3
46. Долгова А.И. Преступность и общество.- М. 1992, - 204с.
47. Ельцин Б.Н. Россия на рубеже эпох. Ежегодное послание Президента // Российская газета, 31 марта 1999г.
48. Жуков А.В., Маркин И.Н., Денисов В.Б. Все о защите коммерческой информации. – М., 1992. - 89с.
49. Зегжда Д.П., Ивашко А.М.Основы безопасности информационных систем. – М.:Горячая линия – Телеком, 2000. - 452с.
50. Измайлов А.М. “Концептуальное проектирование интегрированных систем безопасности // БДИ №4, 1998. - с.14.
51. Казакевич О.Ю. Предприниматель в опасности: способы защиты (практическое руководство для предпринимателей и бизнесменов). Объединение УППИКС, М, 1998, - 256с.
52. Казакевич О.Ю., Конеев Н.В, Максименко В.Г. и др. Предприниматель в опасности: способы защиты. Практическое руководство для предпринимателей и бизнесменов. – М.: Юрфак МГУ, 1992. 119с.
53. Каторин Ю.Ф., Куренков Е.В., А.В.Лысов, А.Н.Остапенко / Энциклопедия промышленного шпионажа / С.Петербург: ООО «Издательство Полигон», 1999. - 512с.
54. Кедровская Л., Ярочкин В. Коммерческая тайна в условиях рыночной экономики. // Информационные ресурсы России. – 1998, №5-6, с.11-15.
55. Кравец Л.Г., Обрезанов С.А. Конкурентоспособность предпринимательства и конкурентная разведка. Изд.дом «Права человека», 2002. - 182с.

56. Кобзарь М.Т., Клайда И.А. Общие критерии оценки безопасности информационных технологий и перспективы их использования//Jet Info.- 1998. - №1.
57. Кобзарь М.Т., Трубачев А.П. Концептуальные основы совершенствования нормативной базы оценки безопасности информационных технологий в России // Безопасность информационных технологий №4, 2000. - с.9-11.
58. Кононов Д.А., Кульба В.В. Формирование сценариев развития макроэкономических процессов на базе использования языка знаковых графов. — // Моделирование экономической динамики: риск, оптимизация, прогнозирование. — М.: МГУ. 1997. - с.7-33.
59. Королев В.И., Морозова Е.В. Методы оценки качества защиты информации при ее автоматизированной обработке // Безопасность информационных технологий №2, 1995. - с.79-87.
60. Кофейников Ю.К. Методы и анализ уязвимости объекта (текущее состояние). Сборник материалов 1-го отраслевого совещания руководителей подразделений безопасности нефтеперерабатывающих и химических предприятий России и СНГ, 2000. - с.34-38.
61. Кульба В.В., Кононов Д.А., Косяченко С.А. Управление безопасностью функционирования сложных систем на основе построения формализованных сценариев их поведения. — //Международная конференция по проблемам управления (29 июня — 2 июля 1999 г.). Избранные труды. Т. 2.. — М.: ИПУ РАН. 1999. - с.26-34.
62. Кульба В.В., Кононов Д.А., Чернов И.В., Шелков А.Б. Методы решения задач обеспечения экономической безопасности государства. — // Проблемы регионального и муниципального управления. Материалы Международной конференции 18 мая 2000г. — М.: РГГУ. 2000. - с.57-58.
63. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М: Новый юрист, 1999. - с.116.
64. Ларичев В.Д. Как уберечься от мошенничества в сфере бизнеса. – М.: Юристъ, 1998, - 216с.
65. Левин В.К -- Защита информации в информационно-вычислительных системах и сетях -- Программирование , №5, 1998. - с.5-16.
66. Лезер Й., Проэктор Д. Революция в политике безопасности. – М., 1996. - 304с.
67. Липаев В.В. Стандарты на страже безопасности информационных систем // PC WEEC/RE.- 2000. - №30.
68. Лукацкий А.В. Адаптивная безопасность сети. Компьютер-Пресс, №8, 1999, с.23-34.
69. Лукацкий А.В. Обнаружение атак.- СПб.: БХВ-Петербург, 2001, - 98с.
70. Макагонова Н.В. О некоторых нерешенных проблемах законодательства по авторскому праву: Заметки практика // Государство и право. - 1996. - №1.
71. Максименко С.В. Технологическая модель обеспечения достоверности данных информационных технологий. // Безопасность информационных технологий. – 1998, №2, - с.14-15.

72. Максимова В.Ф. Микроэкономика. Учебник. Издание третье, переработанное и дополненное – М.: «Соминтэк», 1996, - 328с.
73. Малежин О.Б. Опыт обеспечения информационной безопасности естественных монополий // Сборник материалов конференции «Информационная безопасность России в условиях глобального информационного общества» 18 июня 2001, Москва. – 2001, - с.46-51.
74. Марков С.В. Без защиты информации нет бизнеса.// «Конфидент» №3, 2002. - с.4-6.
75. Материалы семинара Университета МВД РФ. – СПб.: Университет МВД РФ, 1997. - с.18-25.
76. Минна Р. Закон против мафии. Пер. с итал. – М.,1989. - 115с.
77. Мироничев С.Ю. Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы борьбы с ним. М.: Дружок, 1995. - 216с.
78. Мишин Е.Т., Оленин Ю.А., Капитонов А.А. Системы безопасности предприятия – новые акценты // Конверсия в машиностроении№4, 1998. - с.46-51.
79. Общие критерии оценки безопасности информационных технологий: Учебное пособие. Перевод с англ. Сидак Е.А. // Под ред.Кобзаря М.Т., Сидака А.А. – М.: МГУЛ, 2001. - 84с.
80. Орехов С.А. Менеджмент финансово-промышленных групп (учебный курс). Московский государственный университет экономики, статистики и информатики. – М., 2002. – 84с.
81. Орехов С.А., Селезнев В.А. Теория корпоративного управления. // Московский государственный университет экономики, статистики и информатики. – М., 2002. – 148с.
82. Орехов С.А., Агкацева И.Э. Управление финансами корпораций. // Московский государственный университет экономики, статистики и информатики. – М., 2002. – 92с.
83. Осипов В.Ю. Оценка ущерба от несанкционированного доступа к электронно-вычислительной системе. // Безопасность информационных технологий №2, 1995. - с.17-19.
84. Петраков А.В. Основы практической защиты информации. – М.: Радио и связь, 1999. - 368с.
85. Петраков А.В. Защита и охрана личности, собственности, информации: Справочное пособие. – М.: Радио и связь, 1997. - 320с.
86. Петренко С.А., Петренко А.А., Аудит безопасности Intranet. – М.:ДМК Пресс, 2002. - 416с.
87. Петренко С.А., Симонов С.В. Новые инициативы российских компаний в области защиты конфиденциальной информации // Конфидент №1, 2003. - с.34-38.
88. Портер М. Международная конкуренция: Пер.с англ. / Под ред. и с предисловием В.Д.Щетинина. – М.: Международные отношения, 1993. - 345с.
89. Предпринимательство и безопасность. Т.2.Ч.1. – М.:АНТИ, 1991, 346с.

90. Ракитянский Н. Информационная безопасность предприятия. // Информационные ресурсы России №2, 1999. - с.5.
91. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под. Ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. - 376с.
92. Руководство по оценке эффективности инвестиций: Пер. с англ. перераб. и дополн. изд-е. – М.: АОЗТ «Интерэксперт», «ИНФРА-М», 1995.- 98с.
93. Сардак И.Г. Борьба с экономическими преступлениями выходит на новый уровень // М.: Гротек. Системы безопасности связи и телекоммуникаций №3, 1998 - с.13-24.
94. Сергеев А.П. Право интеллектуальной собственности в Российской Федерации. - М.: Теис, 1996.
95. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты.//Конфидент №2, 2001. – с.48-53.
96. Симонов С.В. Методология анализа рисков в информационных системах.// Конфидент №1, 2001. – с.72-76.
97. Симонов С.В. Технологии аудита информационной безопасности.// Конфидент №2, 2002. – с.36-41.
98. Скуратов Ю.И., Лебедев В.М. Комментарий к Уголовному кодексу Российской Федерации – М.: Инфа-М – Норма,1996, - 98с.
99. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.:ДМК Пресс, 2002. - 134с.
100. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю., Серегин В.В. Защита информации в персональных ЭВМ – М.: Радио и связь, «Веста», 1998. - 191с.
101. Спицнадель В.Н. Основы системного анализа: Учебн.пособие. – СПб.: Бизнес-пресс, 2000. - 176с.
102. Степанов Е. «Кроты» на фирме (персонал и конфиденциальная информация)// Предпринимательское право №4, 1999. - с 49.
103. Сырков Б. Компьютерная преступность в России. Современное состояние // Системы безопасности связи и телекоммуникаций. М.: Гротек №4, 1998. – с.36.
104. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий // Под общ. Ред. В.А. Галатенко. – М.:СИП РИА, 2001. - 356с.
105. Тюнина Н.О**.** Анализ причин потерь информации в предпринимательской сфере на основе сбора статистических данных. Теория и практика статистического анализа: Сборник научных трудов./ Московский государственный университет экономики, статистики и информатики. – М., 2002. - с.78-81.
106. Тюнина Н.О. Основы формирования политики безопасности в коммерческой фирме как субъекте предпринимательской деятельности. Организационно-управленческие проблемы трансформации Российской экономики. Сборник трудов Межвузовского научного семинара. / Под ред.: д.э.н. проф. Ильенковой С.В. – М.:ИНИОН РАН, 2002. - с.163-166.

107. Тюнина Н.О. Оценка эффективности применения информационных технологий при подготовке руководителей высшего и среднего звена для современного бизнеса. Роль информационных технологий при обучении на программе МВА: Сборник тезисов докладов.- М.: Издательский центр МЭСИ, 2003. - с.272-276.
108. Фатхутдинов Р.А. Конкурентоспособность: экономика, стратегия, управление. – М.: ИНФРА-М. – 2000. – 312с.
109. Фатхутдинов Р.А. Стратегический маркетинг: Учебник. – М.: БШ, 2000. - 640с.
110. Хриби У., Гэмми Б., Уолл С. Экономика для менеджеров: Учеб.пособие для вузов / Пер. с англ. под ред. А.М. Никитина – М.: ЮНИТИ, 1999. - 535с.
111. Черней Г.А. Моделирование задач оценки эффективности информационной безопасности экономических информационных систем. Автореферат диссертации канд. эконом. наук – М., 1996. - 24с.
112. Чернышева С.А. Авторский договор в гражданском праве России. - М., 1996.
113. Шаваев А.Г. Безопасность копрораций. Криминологические, уголовно-правовые и организационные проблемы. – М.:Концерн «Банковский Деловой Центр», 1998. - с.42.
114. Шанк Дж., Говиндараджан В. Стратегическое управление затратами / Пер. с англ. СПб.: ЗАО «Биснес Микро», 1999. - 288с.
115. Шершеневич Г.Ф. Учебник торгового права / По изд. 1914 г. – М., 1994.
116. Шибалкин О.Ю. Проблемы и методы построения сценариев социально-экономического развития. – М.: Наука, 1992. - 176 с.
117. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия. – СПб: “Алетейя”, 1999. - с.59.
118. Шумпетер Й. Теория экономического развития. – М., 1982. - с.159.
119. Юданов А.Ю. Конкуренция: теория и практика: Учебн. Пособие, 2-е изд. – М.: Гном-Пресс, 1998.
120. Ярочкин В.И. Безопасность информационных систем. – М. Ось-89, 1997 - 320с.
121. Ярочкин В.И. Система безопасности фирмы. – М. Ось-89, 1997. - 192с.
122. Ярочкин В.И. Предприниматель и безопасность. - М., Ось-89, 1994. - 234с.
123. Ярочкин В.И. Секьюритология - наука о безопасности жизнедеятельности. - М.: "Ось-89", 2000. - с.151.
124. A practical guide to the use of CRAMM, 1998.
125. Baker R.H. Computer Security Handbook. Blue Ridge Summit (Pensylvania): TAB Professional Reference Books, 1994.
126. Barker L.K., Nelson L.D. Security standart – gavernment and commercial. // AT&Technical Journal. – 1998, vol.67, № 3, p.9-18.
127. Daly J. Virus vagaries foil feuds. // Computerworld. – 1996, vol.27, №28, p.1,15.
128. Information security management. Part 2. Specification for information security management systems. British Standart BS7799, Part 2, 1998.

129. Information security management: an introduction. DISC PD 3000, 1998.
130. Information security. Handbook – N.Y., 1999.
131. Information Technology Security Evaluation Criteria (ITSEC). Harmonised Criteria of France — Germany — the Netherlands — the United Kingdom -- Department of Trade and Industry, London , 1991.
132. ISO/IEC 15408-1 Information technology – Security technigues – Evaluation criteria for IT security – Part 1: Introduction and general model, 1999.
133. Savka K. Security Resources Planning//Competitive Intelligence Magazine, Sept-Oct 2001.
134. Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800 -- CCITT, Geneva , 1991.
135. Styblinski M.A. Formulation of the drift reliability optimization problem. // Microelectronic Reliab. – 1997, vol.31, №1, p.159-171.
136. Wolfe A.B. Computer Security: For Fun and Profit.// Computer&Security.- 1995, №14, p.113-115.
137. www.agentura.ru/dosie/fapsi/tesis – Тезисы выступления генерального директора ФАПСИ Матюхина В.Г. на открытии Всероссийской конференции «Информационная безопасность России в условиях глобального информационного общества».
138. www.bsi.bund.de/gshb/english/menue.htm - BSI Bundesamt fur Sicherheit in der Informationstechnik.
139. www.cnews.ru – Анализ угроз ИБ. Архив 2001 года. Холдинг РБК.
140. www.home.cris.net/~maikl/Komp/08.htm – Практика защиты коммерческой тайны в США.
141. www.isn.ru/index112.shtml – Анатомия информационной безопасности США. Статья А.Левакова.
142. www.newasp.omskreg.ru/bekryash/lit1 - Электронный учебник «Теневая экономика и экономическая преступность».
143. www.oviont.ru/articles.show.html - Стандарт ISO 17799.
144. www.pcweek.ru/Year2001/N37/CP1251/NetWeek/chapt1.htm - NETWEEK безопасность.
145. www.sssr.h1.ru/3iso15408100.htm – ГОСТ Р ИСО/МЭК 15408-1-2001.
146. www.unix1.jinr.ru/faq_guide/security/jet/analiz_riskov/article1.1.1999.html - UNIXGEMS (статьи по информационной безопасности).
147. www.unix1.jinr.ru/faq_guide/security/jet/infosec/article1.1-3.1996.html - Информационная безопасность. Статья В.Галатенко.
148. www.usp-compulink.ru - Официальный сайт компании «Компьюлинк».
149. www.osp.ru/os/2002/07-08/054_1.htm - Функциональная безопасность корпоративных систем. Статья И.Трифаленкова, Н.Зайцевой.
150. www.iis.ru/library/riss/riss.ru.htm - Концепция формирования информационного общества в России.
151. www.hse.ru/~erussia/default.htm - Федеральная целевая программа "Электронная Россия на 2002-1010 годы."
152. www.iis.ru/library/isp2010/isp2010.ru.html - Концепция федеральной целевой программы "Развитие информатизации в России на период до 2010 года".

153. www.pubs.carnegie.ru/books/2002/08is - Интернет и российское общество. Под редакцией И.Семенова. (Книга).
154. www.netconference.ru/documents/index.asp?id=49# - . Анализ готовности России к вхождению в глобальное информационное общество. Статья А.Короткова.
155. www.pcweek.ru/year1998/n48/cp1251/reviews/chapt4.htm - Россия и глобальное информационное общество. Статья В. Дрожжинова, Ф.Широкова.
156. www.e-commerce.ru – Организация защиты коммерческой тайны.
157. www.OXPAHA.ru - Российские проблемы информационной безопасности.
158. www.scrf.gov.ru/documents/decree/2000/24-1.html- Концепция национальной безопасности РФ.