МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Рубцовский индустриальный институт (филиал)
федерального государственного бюджетного образовательного
учреждения высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»
(РИИ АлтГТУ)

Е.В. Коробкина

БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

КУРС ЛЕКЦИЙ

Учебное пособие для студентов
очной и заочной форм обучения направления
«Менеджмент»

Рекомендовано Рубцовским индустриальным институтом (филиалом) ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова» в качестве учебного пособия для студентов, обучающихся по направлению подготовки «Менеджмент»

Рубцовск 2015

ББК 65.29

Коробкина Е.В. Безопасность предпринимательской деятельности: Курс лекций: Учебное пособие для студентов очной и заочной форм обучения направления «Менеджмент» / Рубцовский индустриальный институт. – Рубцовск, 2015. - 114 с.

В пособии рассматриваются базовые понятия безопасности предпринимательской деятельности, основные направления ее обеспечения, классификация различных видов угроз, обобщаются современные методы управления безопасностью на предприятии. Представлены основные темы дисциплины, требования к выполнению контрольных работ, словарь, учебно-методические материалы. Доступность и краткость изложения позволяют быстро и легко получить основные знания по предмету, подготовиться и успешно сдать зачет.

Учебное пособие предназначено для студентов, обучающихся по направлению «Менеджмент» очной и заочной форм обучения. Пособие разработано в соответствии с ФГОС ВПО направления подготовки «Менеджмент».

Рассмотрено и одобрено
на заседании НМС РИИ.
Протокол № 8 от 26.11.15.

Рецензент:
к.э.н., доцент А.В. Карпенко
юрист ООО «АрКост» И.А. Деревнина

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5
ГЛАВА 1. БЕЗОПАСНОСТЬ И ПРЕДПРИНИМАТЕЛЬСТВО: ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 8
1.1. Предпринимательская деятельность как объект посягательств 8
1.2. Основные понятия безопасности 10
1.3. Комплексная безопасность предприятия 12
ГЛАВА 2. ОПАСНОСТИ И УГРОЗЫ ПРЕДПРИНИМАТЕЛЬСТВУ 14
2.1. Формы взаимоотношений субъектов рынка 14
2.2. Виды экономических угроз 18
2.3. Социальные и политические угрозы 21
2.4. Информационные угрозы 22
2.5. Коррупция как фактор угроз предпринимательству 23
2.6. Правовые угрозы 24
2.7. Криминальные угрозы 25
2.8. Хозяйственные преступления 26
ГЛАВА 3. ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ 26
3.1. Правовая защита 27
3.2. Организационная защита 28
3.3. Инженерно-техническая защита 32
3.4. Универсальные меры обеспечения безопасности предприятия 33
ГЛАВА 4. ОРГАНИЗАЦИЯ СЛУЖБЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ 33
4.1. Цели, задачи, функции службы безопасности 33
4.2. Структура службы безопасности 36
ГЛАВА 5. ОРГАНИЗАЦИЯ РЕЖИМА И ОХРАНЫ 38
5.1. Основные задачи режима и охраны 38
5.2. Требования внутриобъектового режима 40
5.3. Организация пропускного режима 41
5.4. Виды пропусков 44
ГЛАВА 6. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ТРАНСПОРТИРУЕМЫХ ГРУЗОВ ПРЕДПРИЯТИЯ 45
6.1. Общие положения перевозки грузов различными транспортными средствами 45
6.2. Организация охраны грузов на железнодорожном транспорте 47
6.3. Организация охраны грузов, перевозимых автомобильным транспортом 49
6.4. Охрана грузов при использовании воздушного транспорта 50
ГЛАВА 7. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ 50
7.1. Основные направления компьютерных преступлений 51
7.2. Классификация компьютерных преступлений 54

7.3. Защита компьютерных данных 58
ГЛАВА 8. БИЗНЕС - РАЗВЕДКА 61
8.1. Роль разведки в обеспечении экономической безопасности предприятия 61
8.2. Информационные потребности предприятия 62
8.3. Разведка конкурентов 63
8.4. Планирование разведывательной деятельности 66
8.5. Виды и методы разведки 67
8.6. Принципы и технология добывания информации 69
8.7. Определение эффективности добывания информации 73
ГЛАВА 9. КАДРОВАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ 74
9.1. Определение кадровой безопасности предприятия 74
9.2. Особенности отбора персонала 76
9.3. Обеспечение безопасности предприятия при увольнении персонала 86
ВОПРОСЫ К ЗАЧЕТУ по дисциплине «Безопасность предпринимательской деятельности» 89
ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНЫХ РАБОТ по дисциплине «Безопасность предпринимательской деятельности» 90
ВАРИАНТЫ КОНТРОЛЬНЫХ ЗАДАНИЙ по дисциплине «Безопасность предпринимательской деятельности» 92
УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ 97
СЛОВАРЬ 99

ВВЕДЕНИЕ

Современная российская и мировая действительность демонстрирует необходимость разобраться, что из себя реально представляет такая сфера деятельности, как безопасность предпринимательства. Причем сделать это не только в технических и охранных аспектах, но более всего – в организационных, управленческих на основе системного подхода к ним. Поэтому менеджеры и собственники негосударственных субъектов экономики должны быть знакомы с обстоятельствами, обуславливающими их информационную, физическую и имущественную безопасность, и с возможностями, которые предоставляют организационные мероприятия и технические средства (системы) по поддержанию этой безопасности.

Учебное пособие выполнено в форме курса лекций, позволяющего студентам очного и заочного отделений направления *«Менеджмент»* получить базовый объем знаний, выполнить контрольную работу, подготовиться к зачету по дисциплине «Безопасность предпринимательской деятельности». Основные термины представлены в словаре данного пособия, что также облегчает подготовку студентов по данной дисциплине.

Предметом изучения дисциплины «Безопасность предпринимательской деятельности» является система методов разработки решений по достижению поставленных целей в области обеспечения экономической безопасности бизнеса.

В пособии раскрывается содержание понятия «безопасности», способы планирования и организации осуществления мер защиты правового, организационного, экономического, научно-технического и социально-психологического характера, направленных на прогнозирование, отслеживание и учет угроз экономической деятельности предприятия от факторов внешней и внутренней среды с целью обеспечения коммерческого успеха и снижения экономического ущерба. Ставится задача – сформировать у обучающихся четкое представление о создании условий для обеспечения безопасности предпринимательской деятельности.

В результате изучения курса студенты должны *знать*:

- основные понятия безопасности;
- классификации различных видов угроз предпринимательству и способы защиты от них;
- основные направления обеспечения безопасности коммерческого предприятия;
- технологии бизнес – разведки и др.

В результате изучения курса студенты должны *уметь*:

- структурировать информационные ресурсы;
- анализировать уровень защищенности предприятия;
- анализировать деятельность персонала с позиции безопасности предприятия.

Дисциплина «Безопасность предпринимательской деятельности»

относится к циклу дисциплин по выбору (элективных) направления «Менеджмент».

Для изучения дисциплины «Безопасность предпринимательской деятельности» студент должен опираться на знание курсов экономической теории, основ менеджмента и некоторых др.. Дисциплина формирует у студентов комплекс знаний, умений и навыков, необходимых для творческого подхода к дипломному проектированию. Для освоения дисциплины студенты должны обладать базовыми знаниями в области экономики и других общественных наук в рамках курса средней школы.

Дисциплина «Безопасность предпринимательской деятельности» достаточно важная в системе профессиональной подготовки менеджеров, так как формирует у студентов набор знаний и умений по вопросам управления безопасностью и играет важную роль в достижении организацией своих стратегических целей, связанных с обеспечением безопасного существования организации во внешней среде.

Требования к результатам освоения дисциплины

Код компетенции по ФГОС ВПО	Содержание компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОК-3	Способность занимать активную гражданскую позицию	Нормы российского законодательства; сущность, цели и принципы информационной безопасности человека и общества, безопасности предпринима-тельской структуры, направления их практической реализации;	Разрабатывать проекты документов правового характера. Различать основные виды преступлений против предпринима-тельской деятельности	Терминологией и основными понятиями, связанными с безопасностью предпринима-тельской деятельности, а также используемых в законодательстве о защите предпринимательской деятельности

Код компетенции по ФГОС ВПО	Содержание компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:		
		знать	уметь	владеть
ОК-9	Умение использовать нормативно-правовые документы в своей деятельности	Порядок применения и толкования законов и других нормативно-правовых актов в сфере предпринима-тельства, информационно-правовые аспекты безопасности информацион-ных ресурсов, принципы и способы охраны интеллектуаль-ной собственности	Толковать и применять законы и другие нормативно-правовые акты в области защиты прав предпринима-тельской деятельности, анализировать уровень защищенности документов в процессе их движения, рассмотрения, использования и исполнения	Методами сбора нормативной и фактической информации, имеющей значение для реализации правовых норм в соответствующ их сферах профессиональ-ной деятельности, а также методами распознавания различных угроз и подбора персонала

ГЛАВА 1. БЕЗОПАСНОСТЬ И ПРЕДПРИНИМАТЕЛЬСТВО: ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Предпринимательская деятельность как объект посягательств
1.2. Основные понятия безопасности
1.3. Комплексная безопасность предприятия

1.1. Предпринимательская деятельность как объект посягательств

Целью экономической системы любой страны является удовлетворение материальных потребностей общества и рациональное использование материальных и людских ресурсов. Решить эти проблемы призван предприниматель, который, используя определенное сочетание ресурсов (земля, труд, капитал), создает товары и услуги.

Предпринимательская деятельность (предпринимательство) – это инициативная деятельность физического лица или группы лиц, направленная на получение прибыли (дохода) и приумножение собственности в условиях рыночной экономики.

Мотив предпринимательской деятельности включает мотив прибыли: в основе лежит строй мышления, для которого характерно *систематическое и рациональное стремление к законному получению прибыли в рамках своей профессии* (по М. Веберу). Но прибыль в данном случае не является самоцелью, а служит своеобразным критерием успеха – показателем успешности проекта. Сам же предприниматель, по Й. Шумпетеру, стремится, в конечном счете, к свободе и самореализации.

Возможность получения предпринимательской сверхприбыли является одной из основных причин посягательств извне на предпринимателя и его дело.

За последние годы накоплен как положительный, так и отрицательный опыт на пути к цивилизованному рынку. Однако рынок таит в себе много опасностей для добросовестного предпринимателя, действующего в зоне повышенного риска. Предприниматель рискует вложенными финансовыми и материальными средствами, своим временем, трудом, деловой репутацией; берет на себя принятие основных решений в процессе ведения бизнеса, которые определяют направление деятельности предприятия и эффективность его функционирования.

Понятие "риск" применительно к бизнесу может обозначать совершенно разные вещи. В частности, под *риском* может пониматься: *потенциальная возможность (опасность) наступления вероятного события или совокупности событий, вызывающих определенный материальный ущерб.*

Предпринимательский риск (опасность неудачи) оценивается вероятностью возникновения непредвиденных, не предусмотренных проектами и планами потерь экономических ресурсов. Ущерб предпринимательству может быть нанесен в результате обстоятельств объективного (непреодолимого)

характера – стихийного бедствия, техногенной катастрофы, неблагоприятного стечения обстоятельств, просчетов и ошибок самого предпринимателя, нарушения обязательств партнерами и т.д. Предпринимательский риск увеличивается, когда имеется криминальная конкуренция, есть вероятность противоправных посягательств со стороны организованной преступности, недобросовестных конкурентов и несостоятельных партнеров, промышленный шпионаж, посягательства на коммерческую тайну и интеллектуальную собственность. У предпринимателей возникает множество проблем с защитой жизни и интересов своего дела от террористических актов и криминальных посягательств со стороны преступных группировок.

Рейтинг обращений отечественных бизнесменов за помощью в охранные фирмы выглядит следующим образом (по убывающей):

1) Проблема возврата средств (не поступает плата за отгруженный товар, не поступает оплаченный товар, не возвращается в указанный срок кредит).

2) Проблема личной безопасности бизнесменов и членов их семей в связи с угрозами и вымогательством.

3) Хищение грузов на транспорте.

4) Кражи личного имущества в квартирах, офисах, коттеджах, загородных строениях; ограбления; угоны автомобилей.

5) Похищение коммерческой информации (кража документов, их копирование, съем информации с компьютеров и факсов, прослушивание и запись телефонных сообщений, разговоров в помещениях, подкуп сотрудников).

6) Кражи и ограбления в магазинах, складских и производственных помещениях.

7) Порча имущества и товаров. Поджоги.

Рассмотрев статистику обращений отечественных предприятий в охранные фирмы, попробуем понять, как определить, для кого и какой интерес будет представлять деятельность предприятия.

В настоящее время в России деятельностью любого хозяйствующего субъекта в основном интересуются: *государство, конкуренты, криминальные структуры и его собственный персонал.*

Государство в основном контролирует правовую основу деятельности предприятия – зарегистрировано ли предприятие, есть ли лицензии, соответствующая виду деятельности и исправно ли уплачиваются налоги. Кроме того, у правоохранительных органов интерес могут вызвать любые действия предпринимателей, нарушающие действующее законодательство.

У остальных "интересующихся" интерес носит, как правило, сугубо материальный характер.

Интерес *криминальных структур* состоит в том, что если предприятие в силу специфики своей деятельности попадает в зону повышенного интереса криминальных структур, то избежать общения с ними вряд ли удастся.

Давление может возникнуть не только в случае проявления непосредственного интереса к предпринимательской деятельности со стороны

криминальных структур, но и как форма недобросовестной конкуренции.

Дело в том, что часто недобросовестная конкуренция не только осуществляется незаконными методами, но и при этом в качестве средств воздействия использует криминальные структуры.

Кроме того, предприятие, а вернее его финансовые средства, представляют большой интерес и для разного рода мошенников, деятельность которых также можно отнести к криминальной.

Конкуренты всегда проявляют интерес к деятельности предприятия, даже если предприниматель об этом и не догадывается. Вопрос лишь в том – что является предметом столь пристального внимания и какие методы используются для его удовлетворения.

Наиболее вероятно, что интерес вызовут используемые *новые технологии, методы работы, программы расширения и НИОКР* и т.д.

Другое направление проявления повышенного интереса – это *информация по настоящим и предполагаемым партнерам, клиентам, перехват выгодных контрактов и инвестиционных проектов, поставщиков и каналов сбыта*.

Персонал, как правило, интересует стабильность в деятельности организации, так как от этого зависит и стабильность заработной платы. Но бывают и исключения – это те, кто о размере своего дохода заботится сам, но за счет предпринимателя. Основные способы при этом – мошенничество либо воровство.

Статистические данные указывают, что приблизительно 58% известных случаев мошенничества и злоупотреблений совершаются служащими, 30% – менеджерами и 12% – топ-менеджерами и собственниками.

Семейные служащие совершают самое большое количество мошенничеств и злоупотреблений и наносят самый высокий средний ущерб – в 72% случаев. А потери, вызываемые мужчинами, в 4 раза больше потерь, вызываемых женщинами. Средние потери, вызванные виновными с высшим образованием, более чем в пять раз превышают потери, вызванные выпускниками средней школы.

В связи с этим возникает состояние опасности для предпринимательской деятельности.

1.2. Основные понятия безопасности

Опасность – вполне осознаваемая, объективно существующая, но не фатальная вероятность (возможность) негативного воздействия на социальный организм или на что-либо, определяемая наличием объективных и субъективных факторов, обладающих поражающими свойствами, в результате которого может быть причинен какой-либо ущерб, вред, ухудшающий его состояние и/или условия жизнедеятельности и придающий его развитию нежелательные динамику (характер, темпы) или параметры (свойства, формы и т.д.).

Опасность является исходной посылкой при рассмотрении проблем

безопасности. При этом необходимо отличать понятие «опасности» от понятия «угрозы».

Угроза – наиболее конкретная и непосредственная форма опасности, т.е. актуализированная (уже действующая опасность), характеризуемая конкретной формой проявления и способом воздействия или совокупностью условий и факторов, создающих опасность интересам граждан, общества и государства, а также национальным ценностям и национальному образу жизни.

Угрозы – это негативные изменения во внешней политической, экономической или природной среде, которые наносят ощутимый реальный ущерб непосредственно жизненным, политическим, экономическим интересам граждан России и предпринимателей и предприятиям либо потенциальный ущерб государству в целом, его структурным элементам.

Различным видам угроз противопоставляется понятие «безопасность».

В соответствии с определением, приведенным в Законе РФ «О безопасности» от 5 марта 1992 г. №2446-1 (хотя на сегодняшний день закон утратил силу, но определение, данное в нем, все так же актуально), *безопасность* – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Безопасность бывает разных видов.

Безопасность информации: 1) обеспечение защиты информации от случайного или преднамеренного доступа лиц, не имеющих на это права; 2) интегральное свойство информации, характеризующееся конфиденциальностью, целостностью и доступностью; 3) защищенность устройств, процессов, программ: среды и данных, обеспечивающая целостность информации, которая обрабатывается, хранится и передается этими средствами; 4) свойство среды обеспечивать защиту информации.

Безопасность объекта – состояние защищенности объекта от различных угроз, при котором созданы условия для его нормального функционирования и строгого соблюдения на нем установленных режимов. Безопасность объекта обеспечивается и поддерживается путем разработки и реализации системы мер, осуществляемых администрацией объекта.

Безопасность (защищенность) предпринимательства – это такое *состояние цивилизованного бизнеса,* при котором отсутствует экономический или иной ущерб, который наносился бы бизнесу преднамеренно или непреднамеренно физическими лицами или социальными организациями (в том числе юридическими лицами) с нарушением закона или этики предпринимательства.

Безопасность коммерческого предприятия – состояние защищенности жизненно важных интересов владельцев, руководства и клиентов предприятия, материальных ценностей и информационных ресурсов от недобросовестной конкуренции, противоправной деятельности криминальных формирований и отдельных лиц, способность противостоять внешним и внутренним угрозам, сохранять стабильность функционирования и развития предприятия в соответствии с его уставными целями.

Экономическая безопасность предприятия – состояние юридических, производственных отношений и организационных связей, материальных и интеллектуальных ресурсов, при которых обеспечивается стабильность функционирования, финансово-коммерческий успех, прогрессивное научно-техническое и социальное развитие.

Таким образом, под *безопасностью предпринимательской деятельности* понимается такое ее *состояние, которое позволяет хозяйствующим субъектам противостоять различным видам угроз, рисков, опасностей и обеспечивает им стабильное, устойчивое и независимое развитие.*

1.3. Комплексная безопасность предприятия

Управление безопасностью – это деятельность менеджера по учету всех возможных взаимосвязей в условиях неопределенности при принятии и выполнении финансовых, организационных и т.п. решений.

Концепция обеспечения безопасности хозяйствующего субъекта – это комплексное, системное видение путей устранения опасностей, которые грозят или могут грозить ему извне, и ликвидация опасностей, которые угрожают ему изнутри.

Создание и реализация концепции безопасности позволяет разрабатывать систему последовательных практических действий по обеспечению внешней и внутренней безопасности хозяйствующего субъекта с учетом его организационного, технического, правового, финансового, информационного и специального назначения.

Систему безопасности предприятия можно определить как рациональную совокупность специальных органов, направлений, средств, методов и мероприятий, обеспечивающих безопасность предприятия, под которой следует понимать состояние защищенности жизненно важных интересов предприятия от источников внутренних и внешних угроз.

Целью обеспечения безопасности предприятия является ограждение его собственности и сотрудников от источников внешних и внутренних угроз, предотвращение правонарушений, причин и условий, их порождающих, а также возникновения чрезвычайных ситуаций. Под угрозой безопасности следует понимать совокупность условий и факторов, создающих опасность жизненно важным интересам предприятия. Реальные и потенциальные угрозы объектам безопасности, исходящие от внешних и внутренних источников опасности, определяют содержание деятельности системы безопасности предприятия.

С позиций системного подхода к безопасности предъявляются следующие *требования.*

Безопасность должна быть:

- *непрерывной.* Это требование проистекает из того, что злоумышленники всегда ищут возможность обойти защиту для своих противоправных действий;

- *целенаправленной и конкретной.* Защищается то, что должно защищаться в интересах конкретного предприятия, а не все подряд;
- *централизованной.* В рамках определенной структуры должна обеспечиваться организационно-функциональная самостоятельность процесса обеспечения безопасности предприятия;
- *плановой.* Планирование осуществляется путем разработки детальных планов действий по обеспечению защищенности предприятия всеми компонентами его структуры;
- *активной.* Защитные меры претворяются в жизнь с достаточной степенью настойчивости;
- *надежной.* Методы, средства и формы защиты должны надежно перекрывать все пути проникновения и возможные каналы утечки информации. При этом надежность предполагает не только перекрытие, но и дублирование средств и мер безопасности;
- *универсальной.* Меры безопасности должны надежно перекрывать пути угроз независимо от места их возможного воздействия;
- *комплексной.* Комплексный характер защиты проистекает из того, что это специфическое явление, представляющее собой сложную систему непрерывно взаимосвязанных и взаимозависимых процессов, каждый из которых, в свою очередь, имеет множество различных взаимообусловливающих друг друга сторон, свойств и тенденций. Для обеспечения безопасности во всем многообразии структурных элементов, угроз и каналов несанкционированного доступа должны применяться все виды и формы защиты в полном объеме. Недопустимо применять отдельные формы или технические средства.

Как состояние безопасность определяется такими критериями, как отсутствие реальной угрозы для хозяйствующего субъекта со стороны внешних и (или) внутренних деструктивных факторов и наличием у хозяйствующего субъекта сил, средств и ресурсов противостоять им.

Такая трактовка комплексной безопасности фирмы позволяет руководителю службы безопасности фирмы, частного охранного предприятия определить цели обеспечения безопасности фирмы, которые вытекают из:

1. Главных направлений деятельности фирмы.
2. Потенциальных и реально существующих факторов внешней и внутренней угрозы для фирмы.

Для обеспечения комплексной безопасности фирмы необходимо решать следующие вопросы:

- противодействие факторам внешней угрозы фирмы, недобросовестным партнерам, конкурентам, включая защиту от преступного мира;
- обеспечение безопасности фирмы от противоправных действий представителей контролирующих органов;
- внутренней безопасности фирмы, связанной с защитой ее интересов от возможных противоправных действий со стороны некоторых ее руководителей и (или) сотрудников;

• профилактика возможных нарушений закона (ов) со стороны самой фирмы по отношению к другим субъектам предпринимательской деятельности (как физическим, так и юридическим лицам);

• взаимодействие с правоохранительными и контролирующими органами в целях предупреждения и пресечения правонарушений, направленных против интересов фирмы;

• организация защиты и проведение мер по предотвращению чрезвычайных ситуаций.

Вместе с тем важно, чтобы перечисленные выше вопросы обеспечения безопасности комплексно реализовывались в следующих секторах безопасного функционирования фирмы.

1. Производственно-технологическом секторе (сохранность технологических процессов, материальных ценностей).

2. Коммерческо-правовом (анализ и оценка партнера, юридическая защита интересов фирмы, обеспечение безопасной динамики финансовых и материальных ресурсов фирмы).

3. Информационном секторе (определение важности информации, обеспечение противодействия угрозам информации, которые выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности).

4. Кадровом секторе (подбор и расстановка кадров в соответствии с их умением обеспечить эффективную и безопасную работу фирмы).

Выявление основных секторов безопасного функционирования дает возможность определить основные формы и способы защиты интересов фирмы (предпринимателя) практически по всем направлениям безопасного ведения бизнеса.

ГЛАВА 2. ОПАСНОСТИ И УГРОЗЫ ПРЕДПРИНИМАТЕЛЬСТВУ

2.1. Формы взаимоотношений субъектов рынка
2.2. Виды экономических угроз
2.3. Социальные и политические угрозы
2.4. Информационные угрозы
2.5. Коррупция как фактор угроз предпринимательству
2.6. Правовые угрозы
2.7. Криминальные угрозы
2.8. Хозяйственные преступления

2.1. Формы взаимоотношений субъектов рыка

Говоря об экономических угрозах, необходимо отметить, что отношения между производителями в условиях рыночной экономики могут быть охарактеризованы степенью доброжелательности, взаимной терпимости, взаимного участия в делах, с одной стороны, и явно настороженными, грубыми, активно противоборствующими – с другой.

Полярными в этой ситуации выступают отношения тесного *сотрудничества* и *противоборства*. Между этими крайними формами отношений можно выделить по степени нарастания напряженности такие формы отношений, как *взаимодействие, соперничество, конкуренция.*

Таблица 2.1

Характер отношений с конкурентами

Форма конкурентных отношений	*Характер конкурентных отношений*	*Оценка деловой обстановки*
сотрудничество	доброжелательные	благоприятная
взаимодействие	разногласия	осложненная
соперничество	противоречия	сложная, противоречивая
конкуренция	угрожающие	конфликтная
противоборство	конфронтационные	остроконфликтная

Сотрудничество. Содержанием сотрудничества являются широкие совместные действия фирм в достижении высоких прибылей в процессе производства и продажи своей продукции.

Сотрудничество проявляется в тесных деловых отношениях со своими партнерами. Наиболее ярко оно проявляется в отношениях с поставщиками.

В условиях насыщения рынка и чрезмерно жесткой конкуренции покупатели теряются в массе предложений, рекламы и антирекламы. При таком положении отдельные фирмы стремятся к сотрудничеству. Объединение мощных компаний, ранее находившихся в состоянии противостояния, приводит к взаимовыгодной деятельности. Наилучшим сотрудничество бывает, когда реализуются общие интересы. Развитие отношений в экономике, особенно на мировом уровне, во многом зависит от того, насколько глубоко стороны осознают, что живут в тесном взаимозависимом мире, в котором можно достичь собственных интересов лишь путем эффективного сотрудничества.

Взаимодействие – форма отношений, отличающихся согласованностью действий по цели, месту и времени для достижения максимального эффекта и получения максимальной прибыли при производстве и сбыте товаров.

Взаимодействие предполагает взаимность как один из основных принципов взаимоотношений сторон, базирующихся на правовых нормах.

Взаимодействие по степени ослабления связей или по степени возрастания напряженности в отношениях сторон хотя и стоит на втором месте, все же соответствует добрососедским отношениям.

Альтернативой взаимодействию может быть достижение всеми участниками баланса интересов, который в цивилизованном рыночном хозяйстве должен представлять собой баланс между сотрудничеством и соперничеством.

Соперничество – антагонистические действия в достижении превосходства над конкурентом или противной стороной.

Борьба за внешние рынки и сферы приложения капитала, будучи в современн6ых условиях главным орудием соперничества, выступает одним из

важнейших факторов острых противоречий и конкурентной борьбы.

Соперничеству в современных условиях свойственны: открытая враждебность, повышенная бдительность и взаимная агрессивность.

Конкуренция. Конкуренцию можно определить как антагонистическую борьбу за более выгодные условия производства и сбыта, за получение наибольшей прибыли, достижение которых ведется различными путями, вплоть до сбивания цен на продукцию.

Наиболее опасной считается недобросовестная конкуренция, связанная с нарушением принятых норм и правил.

В рамках добросовестной конкуренции для достижения своих целей фирмы предпринимают активные действия: постоянно совершенствуют стратегию и тактику деятельности, автоматизируют производство, улучшают структуру управления, реализуют программы по активному вовлечению работников в управление, увязывают размер оплаты с эффективностью труда, улучшают качество выпускаемой продукции.

Противоборство – острая антагонистическая борьба за завоевание и монопольное владение рынком сбыта.

На этой фазе отношений применяются самые различные меры с целью нанесения конкуренту значительного материального ущерба вплоть до захвата, убийства сотрудников, взрывов и поджогов и т.п.

Одной из наиболее распространенных форм противоборства является *рейдерство.*

Рейдерство является сложнодоказуемым, «интеллектуальным» видом преступлений, распространенным в различных странах. Однако в государствах с развитой рыночной экономикой, стабильным законодательством, невысоким уровнем коррупции и цивилизованными предпринимательскими традициями рейдерство находится на периферии, не превращаясь в системную проблему. Рейдеры являются ловкими маргиналами, стремящимися к быстрой наживе, но не становящимися «персонами грата» в элите. В странах с «переходными» экономиками ситуация часто является иной – незаконный передел собственности носит системный характер и представляет значительную угрозу.

В американской практике рейдерство традиционно делится на три типа:

- *«черное» рейдерство* – использование исключительно незаконных действий для установления контроля над предприятием: шантаж, подкуп, силовой вход на предприятие, подделка судебных решений, реестра акционеров и так далее.
- *«серое» рейдерство* – сочетание квазизаконных и незаконных мер: подкуп судей для ускорения принятия законного решения на основании поддельного реестра акционеров, шантаж контрагентов предприятия для создания ситуации невозможности продолжения деятельности и так далее.
- *«белое» рейдерство* – квазизаконные действия: срыв собрания акционеров, использование пробелов в законодательстве, забастовки, организация проверок контролирующими органами. Нетрудно заметить, что и «белое» рейдерство, на первый взгляд, более соответствующее законным

нормам, чем первые два типа, также часто связано с нарушениями действующего законодательства. Например, при организации забастовок подкупаются руководители профсоюзов, а при инициировании проверок – сотрудники контролирующих организаций.

В последние годы рейдерство в России, опираясь на административный ресурс и коррумпированные правоохранительные органы в своих методах, становится проще, на место многоходовых схем приходят более простые приемы. Оно становится более похожим на «беловоротничковый» уголовный промысел, совершаемый организованными преступными группами. С одной стороны, подобные тенденции ведут к еще большей криминализации данного явления, что повышает его общественную опасность. С другой стороны, упрощение рейдерских схем помогает этим явлением – разумеется, при наличии достаточной политической воли.

По данным Интернет-энциклопедии «Википедия», существуют четыре основных способа захвата предприятия:

- через акционерный капитал: рейдеры скупают миноритарный пакет акций. Обычно этого достаточно для того, чтобы инициировать собрание собственников и принять нужное решение, например, смену руководства. В ряде случаев речь идет не о захвате предприятия, а о принуждении мажоритарных акционеров к выкупу у миноритариев их пакета акций по завышенной цене;
- через наемное руководство: менеджмент может просто «выводить» активы на подконтрольные рейдеру структуры или брать кредиты под залог собственности под нереальные проценты;
- через кредиторскую задолженность: если у предприятия имеется несколько относительно мелких задолженностей, рейдер скупает их и предъявляет к единовременной оплате;
- путем оспаривания приватизации: условия для такого рейдерства создаются в тот момент, когда предприятие приватизируется незаконно.

В России особенно распространены два первых способа, которые носят явно криминализированный характер. Третий способ соответствует закону, но является достаточно редким, так как может быть применен только в отношении компаний, ведущих крайне неосторожную кредитную политику. Четвертый способ является нечастым в связи с тем, что основной период российской приватизации пришелся на 1990-е годы и сроки давности по приватизационным сделкам, в основном, уже истекли. Кроме того, доказать незаконность приватизации часто непросто – не случайно, что государство в своей операции против ЮКОСа использовало не этот напрашивавшийся прием, а налоговые обвинения.

Впрочем, в ряде случаев такой способ действует, но в комбинации с другими. Именно сочетание различных приемов делает рейдерские захваты наиболее опасными – тем более, что для него необходимо сочетание различных ресурсов, от административного до финансового.

2.2. Виды экономических угроз

К группе угроз безопасности и преступлений, совершаемых в сфере экономики, относятся: хищения, совершаемые путем присвоения, растраты, злоупотребления служебным положением; кражи; взяточничество; корыстные злоупотребления властью или служебным положением; контрабанда; нарушение правил валютных операций и др. В структуре экономической преступности треть занимают хищения государственного и общественного имущества, совершаемые путем присвоения, растраты либо злоупотребления служебным положением.

Высокую общественную опасность представляют должностные преступления и прежде всего взяточничество, поразившее все звенья управленческих, хозяйственных и коммерческих структур.

Экономическая безопасность предпринимательства определяется современным характером, ориентацией и направленностью воздействующих на него (предпринимательство) внешних и внутренних угроз.

К внешним угрозам относятся:

1. Разведывательная деятельность иностранных спецслужб и организаций.

2. Деятельность иностранных организаций, фирм, компаний, направленная на ущерб национальным интересам и безопасности России.

3. Проникновение в экономику России международных преступных формирований и их капитала.

К внутренним угрозам относятся:

1. Постоянное расширение масштабов коррупции в органах государственной власти, проникновение в них преступных элементов, что, в свою очередь, влияет на развитие негативных тенденций в сферах приватизации, финансово-банковской деятельности в сфере внешнеэкономических связей.

2. Рост экономической преступности, включая контрабанду и незаконный экспорт капиталов, валюты, стратегического сырья, преступления в финансовой сфере, фальшивомонетничество и незаконные операции с ценными бумагами, по привлечению вкладов.

3. Организованная преступная деятельность в экономике, проникновение криминального капитала в важнейшие и наиболее доходные сферы легального бизнеса.

Наряду с макроэкономической существует и микроэкономическая трактовка угроз предпринимательству. По отношению к отдельному предприятию или отдельной коммерческой структуре можно привести следующие виды внешних угроз:

1. Недобросовестная конкуренция.

2. Преступные действия, криминальные насилия, посягательства на коммерческую тайну.

3. Противоправные действия отдельных лиц и организаций административного аппарата, в том числе и налоговых служб.

4. Нарушение установленного регламента сбора, обработки и передачи информации.

5. Промышленный шпионаж.

Внутренние угрозы можно классифицировать следующим образом:

- Преднамеренные преступные действия собственного персонала из-за низкого профессионализма и недобросовестности.
- Непреднамеренные действия и ошибки персонала.
- Отказ оборудования и технических средств.
- Сбои программного обеспечения средств обработки информации.

Объектами различных угроз предпринимательству выступают:

1. Люди (персонал, сотрудники, компаньоны и др.).
2. Материальные ценности.
3. Финансовые ресурсы.
4. Информационные ресурсы, включая патенты, незавершенные проектно-конструкторские разработки, программные продукты, массивы бухгалтерской и статистической информации и пр.

В условиях сохраняющейся высокой степени монополизации российской экономики большую опасность в плане производства (продуцирования) экономических угроз предпринимательству, особенно малому, представляет практика недобросовестной конкуренции.

Под *недобросовестной конкуренцией* понимают действия, направленные на приобретение преимущества в предпринимательской деятельности хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и могут причинить убытки другим хозяйствующим субъектам – конкурентам либо нанести ущерб их деловой репутации.

В более широком плане *недобросовестная конкуренция* – это любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства и способны причинить ущерб субъектам рынка.

Основной принцип недобросовестной конкуренции заключается в стремлении закрепить свое положение на рынке за счет ослабления позиций конкурентов или обмана потребителей. Для этого на конкурирующие фирмы оказывается соответствующее давление, которое может осуществляться в прямом или косвенном виде.

К числу таких действий принято относить:

- использование своего экономического потенциала для продажи продукции по ценам ниже себестоимости (демпинг) с целью подрыва позиций конкурента и последующего вытеснения его с рынка.

Демпинг – продажа товаров на внешнем и внутреннем рынках по искусственно заниженным ценам, меньшим средних розничных цен, а иногда и более низким, чем себестоимость (издержки производства и обращения).

Демпинг проводится с целью проникновения на рынок, завоевания места на нем, вытеснения конкурентов. Демпинг осуществляется государством и компаниями в расчете на возмещение в будущем текущих убытков, когда за счет демпинга будет достигнуто прочное положение на рынке. Однако довольно часто и фирмы, и государство прибегают к демпингу как разовому мероприятию, способу быстрого получения необходимых денежных, валютных средств. В мировой экономической практике, в ряде стран принято противостоять демпингу путем применения антидемпинговых законов, установления специальных противодемпинговых пошлин.

- злоупотребление господствующим положением на рынке (монополия);
- установление дискриминационных коммерческих условий;
- тайный сговор на торгах и неофициальное создание тайных картелей;
- выпуск продукции с характеристиками, не соответствующими рекламе;
- подделка и производство оригинальных изделий, выпускаемых конкурентами;
- незаконное использование товарных знаков для маркировки своей продукции.

Значительную угрозу предпринимательству несет *мошенничество* – завладение чужим имуществом или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Способы завладения имуществом при мошенничестве своеобразны: преступник прибегает к обману лиц, во владении или ведении которых оно находится, в результате чего они, будучи введенными в заблуждение, добровольно передают имущество преступнику, полагая, что последний имеет право его получать.

При совершении мошенничества обман выступает в качестве одного из элементов совершения преступления, является необходимым признаком, обуславливающим неправомерный переход имущества из владения правомочного лица в незаконное владение преступника.

Цель мошенничества – ввести в заблуждение владельца имущества и добиться добровольной передачи его в распоряжение преступника.

Широкое распространение получило *лжепредпринимательство* – создание предпринимательских организаций без намерения осуществлять уставную деятельность с целью получения кредитов, снижения налогообложения или иного извлечения имущественной выгоды противозаконным путем.

Заметно растет количество злоупотреблений в финансово-кредитной сфере, среди которых можно выделить: получение кредита обманным путем; выпуск и распространение необеспеченных ценных бумаг, а также нарушение порядка их эмиссии; незаконные операции по переводу за границу значительных денежных сумм; подделка банковских чеков и кредитных карточек.

Значительную общественную опасность представляют *ложное и злостное банкротство* – заведомо ложное заявление предпринимателя о невозможности исполнения обязательств перед кредиторами с корыстными целями, а также умышленное сокрытие предпринимателем-должником своей устойчивой

неплатежеспособности путем предоставления сведений, не соответствующих действительности.

Говоря об экономической безопасности, необходимо установить взаимосвязь угроз со стороны конкурентов и злоумышленников и рисков в процессе функционирования предприятия во времени и в пространстве угроз. Пространство угроз охватывает объект защиты – персонал коммерческой структуры, имущество, денежные средства и сведения, составляющие коммерческую или служебную тайну. Каждая угроза влечет за собой определенный ущерб – моральный или материальный, а противодействие призвано снизить его величину, в идеале полностью.

2.3. Социальные и политические угрозы

Социальные угрозы связаны с повышением уровня безработицы, расширяющейся зоной нищеты, увеличивающимся разрывом в уровнях доходов между бедными и богатыми, с нарастающей региональной дифференциацией. Сюда же можно отнести дискриминационное положение женщин в бизнесе, инвалидов, военнослужащих и т.д.

Социальные угрозы предпринимательству вызваны в значительной степени сохраняющейся в стране экономической и политической нестабильностью, что порождает безработицу, нищету, социально-экономическое расслоение общества в связи с разрывом в уровнях доходов и в еще большей мере – в располагаемых имущественных и финансовых ресурсах. Применительно к предпринимательству эти обстоятельства затрудняют вхождение в бизнес широких слоев населения. Нестабильность функционирования предприятий малого и среднего бизнеса приводит к разорению, банкротству многих из них, что также дополнительно порождает безработицу. Затрудненность и неравная доступность «вхождения в бизнес» для различных социальных групп населения порождает дополнительную напряженность в обществе, генерирует негативное, а часто и криминальное отношение ко всей предпринимательской среде.

Угрозы предпринимателям усиливаются в связи с тем, что часто под контролем различных общественных и благотворительных организаций и фондов, создающихся людьми, нуждающимися в защите и поддержке государства, рано или поздно оказываются представители криминально-предпринимательских кругов, легализующих таким образом свои капиталы и получающие дополнительную выгоду за счет предоставляемых данным организациям и фондам налоговых и иных льгот.

Социальные угрозы можно классифицировать по следующим признакам:

- по направленности против социальных интересов предпринимателей;
- по масштабам (местные, локальные, в масштабе предприятия, фирмы);
- по причинам (несправедливое распределение собственности, доходов, жизненных благ, власти и т.д.).

Политические угрозы предпринимательству вызываются

межнациональными конфликтами, их переходом в стадию высокой напряженности и конфронтации. В ряде случаев политическая нестабильность связана с конфликтами исполнительной и законодательной властей на местах, которые втягивают в сферу конфликта и предпринимательские круги. Политическая ситуация в регионе является одним из факторов, определяющих его инвестиционный климат, в зависимости от которого инвесторы, особенно иностранные, принимают решения о вложении своих капиталов в те или иные сферы региональной экономики.

2.4. Информационные угрозы

К группе *информационных угроз* относятся действия, приводящие к ознакомлению с конфиденциальной информацией, к ее модификации (т.е. изменению содержания и структуры в интересах злоумышленника) и к уничтожению, а также действия, приводящие к неправомерному обладанию охраняемыми сведениями, к которым относится разглашение, утечка по техническим каналам и несанкционированный доступ со стороны злоумышленников.

Информация – это сведения о лицах, предметах, явлениях и процессах (независимо от формы их представления), отраженные на материальных носителях, используемые в целях получения знаний и практических решений. Информация выступает как один из важнейших ресурсов, в том числе и предпринимательских. Информация выступает как собственность, она имеет потребительское и стоимостное содержание.

По отношению к информации, к информационным ресурсам можно представить следующие виды угроз:

- ознакомление с конфиденциальной информацией различными путями;
- модификация информации в интересах злоумышленника;
- разрушение информации.

Осуществление этих видов угроз может быть реализовано:

- путем неофициального доступа к источникам конфиденциальной информации;
- путем подкупа сотрудников предприятия, непосредственно связанных с конфиденциальной информацией;
- путем перехвата информации, передаваемой средствами связи или излучаемой различными техническими средствами;
- через переговорные процессы между представителями различных структур.

Угрозы информационного характера для предпринимательства можно также классифицировать на внутренние и внешние.

К внутренним угрозам относятся:

- преднамеренные или случайные негативные воздействия на информационные ресурсы предпринимательских структур, выражающиеся в неправомерном ознакомлении со сведениями, составляющими коммерческую

тайну и иные секреты предпринимателей;

- изменение (фальсификация) состава и структуры информации (баз данных) в преступных целях или ее полное разрушение с целью нанесения предпринимательству морального и материального ущерба;
- разглашение конфиденциальных сведений сотрудниками предприятия как по неосторожности, так и умышленно;
- утечка информации по техническим каналам.

К внешним угрозам относится – недоступность или недостаточная доступность предпринимателей к официальной информации о новых законодательных и иных нормативных актах, в частности в области лицензирования хозяйственной деятельности, налоговой политики, льгот и преимуществ для субъектов малого предпринимательства.

К внешним угрозам в области информации относится:

- недобросовестная конкуренция, проявляющаяся в форме промышленного шпионажа, распространение ложной информации о продукции конкурентов и их финансовом положении;
- в виде несанкционированного доступа к конфиденциальной информации предпринимателей-конкурентов различными легальными и нелегальными путями.

Как внутренние, так и внешние угрозы наносят предпринимателям те или иные виды ущерба в их производственно-коммерческой деятельности.

2.5. Коррупция как фактор угроз предпринимательству

Масштабная коррупция на всех уровнях оказывает разлагающее влияние на все стороны жизни и деятельности страны, в том числе и на малый и средний бизнес.

Негативные последствия проявляются во всех сферах. Например, в экономической сфере это влияние проявляется в следующих видах:

1. Расширяется теневая экономика.
2. Нарушаются реальные конкурентные механизмы рынка.
3. Повышаются цены за счет коррупционных «накладных расходов».
4. Теряется доверие участников рынка к способности власти устанавливать и соблюдать честные правила рыночных отношений.
5. Расширяются масштабы коррупции в неправительственных структурах.

Социальные последствия коррупции:

1. Закрепляется и увеличивается резкое имущественное неравенство, бедность большей части населения.
2. Коррумпированность правоохранительных органов способствует укреплению организованной преступности. Последняя сращивается с коррумпированными группами чиновников и предпринимателей, еще больше усиливается с помощью доступа к политической власти и возможностям отмывания денег.
3. Увеличивается социальная напряженность.

Политические последствия:

1. Уменьшается доверие к органам власти.
2. Растет угроза экономической и политической изоляции на международном рынке.
3. Увеличиваются возможности властвования олигархических группировок.

Можно утверждать, что коррупция, ее масштабы, специфика и динамика – следствие общих политических, социальных и экономических проблем страны.

2.6. Правовые угрозы

Угрозы *правового характера* вызваны, прежде всего, отсутствием устойчивого, исчерпывающего и непротиворечивого законодательства, прежде всего регулирующего процесс хозяйственной деятельности. Наличие «пробелов» в действующем законодательстве и других нормативных документах порождает различные «лазейки» для утаивания прибыли, реальных доходов, различных «обходных маневров» в хозяйственных и финансовых операциях, а также для прямого криминального давления на предпринимательство.

Массовый характер приобрели прямые нарушения местными органами власти законов о предпринимательской деятельности.

Основными видами нарушений являются:

- посягательство на имущество предпринимателей;
- ограничения на межрегиональное перемещение товаров;
- незаконное регулирование цен;
- взыскание не предусмотренных законодательством сборов;
- вмешательство во внутренние дела предприятий;
- попытки административного регулирования деятельности предприятий.

Определенные правовые угрозы (угрозы административного произвола) содержатся и в правовом регулировании практики лицензирования хозяйственной деятельности. Несмотря на Закон РФ «О лицензировании отдельных видов деятельности» от 16 декабря 1998 года, остаются значительные сферы административно-правовых угроз в области предпринимательства. По сути дела под видом лицензирования часто определяется сертификация помещений, в некоторых случаях лицензии выдавались и выдаются на месяц, квартал, полгода. В связи с этим для продления лицензии предприниматель вынужден обходить множество инстанций и везде платить как официальные, так и «неофициальные» сборы.

Для российского предпринимателя угрозы безопасности от существующей практики налогообложения возникают вследствие запутанности ныне действующего законодательства, его нестабильности, возможности, с одной стороны, разнообразных уклонений от налогообложения, а с другой – завышения некоторых налоговых ставок и ненужности целого ряда налогов, а

также неопределенности в налогово-бюджетных взаимоотношениях федерального центра с регионами.

Нестабильность налогового законодательства создает ряд рисковых ситуаций и для зарубежных предпринимателей.

2.7. Криминальные угрозы

Криминальные угрозы генерируются тем, что крупные суммы денег, добытые незаконным путем, вынуждают преступные группировки искать способы их легализации. Преступные группировки все чаще заставляют предпринимателей «принимать в оборот» свои теневые капиталы и отдавать ту или иную меру контроля над предприятием.

В последнее время с развитием коммуникаций и электронных форм расчетов распространились проникновения в компьютерные сети для внедрения фиктивных платежных документов, хищения средств с использованием векселей, арбитражных приказов, акций и облигаций.

Распространение «электронных преступлений» объясняется и довольно низкой степенью защиты компьютерных сетей, и возросшей «квалификаций» мошенников.

Факторы, способствующие распространению криминальных угроз

Внешние:

- объективный рост террористических проявлений в странах ближнего и дальнего зарубежья;
- социально-политическая и экономическая нестабильность в сопредельных государствах, наличие вооруженных конфликтов в отдельных из них;
- стратегические установки некоторых иностранных спецслужб и зарубежных террористических организаций;
- «прозрачность» границ и отсутствие надежного контроля над режимом въезда-выезда;
- наличие каналов нелегального поступления в Россию из-за рубежа оружия, взрывчатых веществ и других, запрещенных для оборота вещей и предметов;
- образование российской «диаспоры» за пределами России.

Внутренние:

- наличие в стране значительного нелегального рынка оружия и относительная легкость его приобретения;
- существенное ослабление ряда административных режимов;
- наличие и деятельность ряда экстремистских группировок;
- обостренное чувство социальной неустроенности и незащищенности;
- слабая работа правоохранительных органов и организаций по защите граждан.

2.8. Хозяйственные преступления

Хозяйственные преступления разделяются на три основные группы в зависимости от защищаемых интересов:

1. Преступления, причиняющие ущерб или создающие реальную возможность причинения ущерба путем непосредственного нарушения интересов государства или любого иного хозяйствующего субъекта, независимо от формы собственности.
2. Преступления, причиняющие ущерб или создающие реальную возможность причинения ущерба путем нарушения интересов граждан, поскольку они соприкасаются с хозяйственной деятельностью учреждений и частных лиц.
3. Преступления, которые могут причинить ущерб народному хозяйству в области его ведения и организации как путем непосредственного нарушения интересов государства или иного хозяйствующего субъекта, так и путем нарушения интересов граждан, поскольку они соприкасаются с хозяйственной деятельностью учреждений и частных лиц.

Хозяйственные преступления ориентированы на следующие сферы деятельности:

1. Преступления в сфере предпринимательской деятельности.
2. Преступления, связанные с нарушением антимонопольного законодательства и законов, запрещающих практику недобросовестной конкуренции.
3. Преступления в сфере защиты прав потребителей.
4. Преступления в налоговой сфере.
5. Валютные преступления.
6. Преступления в финансово-кредитной сфере.
7. Преступления в сфере осуществления внешнеэкономической деятельности.

ГЛАВА 3. ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

3.1. Правовая защита
3.2. Организационная защита
3.3. Инженерно-техническая защита
3.4. Универсальные меры обеспечения безопасности предприятия

Безопасность коммерческого предприятия достигается проведением единой политики в области обеспечения безопасности, системой мер правового, организационного и технического характера, адекватных угрозам жизненно важным интересам предприятия.

Для создания и поддержания необходимого уровня защищенности объектов предприятия разрабатывается система правовых норм, регулирующих

отношения сотрудников в сфере безопасности, определяются основные направления деятельности в данной области, формируются органы обеспечения безопасности и механизмы контроля и надзора за их деятельностью.

Основными *принципами обеспечения безопасности* являются:

- законность;
- соблюдение баланса интересов личности и предприятия;
- взаимная ответственность персонала и руководства;
- взаимодействие с государственными структурами безопасности.

Основными направлениями обеспечения безопасности предприятия как нормативно-правовыми категориями, определяющими комплексные меры защиты его интересов, выступают правовая, организационная и инженерно-техническая защита.

3.1. Правовая защита

Правовые или законодательные основы обеспечения безопасности коммерческого предприятия составляют Конституция РФ, Законы РФ и другие нормативные акты РФ, регулирующие отношения в области безопасности.

Законодательные акты, защищающие интересы личности, материальные и финансовые ресурсы как собственность лица или предприятия, не являются новыми для предпринимателей России. На это направлены Законы и Кодексы, в том числе Уголовный кодекс РФ, четко определяющий понятие, разновидности и состав преступлений против личности, предприятия и государства, различные действия и меры их пресечения.

В части *коммерческой информации* – сведений, связанных с производством, используемой технологией изготовления продукции, управлением, финансами и другой деятельностью предприятия. Формой обеспечения безопасности выступает *коммерческая тайна.*

Коммерческая тайна – форма обеспечения безопасности наиболее важной, наиболее ценной коммерческой информации, составляющей объект охраны и предполагающей ограничения ее распространения.

В зависимости от характера информации, ее доступности для заинтересованных лиц, а также экономической целесообразности конкретных защитных мер, могут быть избраны следующие формы защиты информации:

- признание сведений коммерческой тайной;
- патентование;
- использование норм авторского права;
- использование норм обязательного права.

Необходимо четко понимать, что любые системы защиты информации без создания правовых основ обеспечения безопасности, любые последующие претензии к недобросовестным сотрудникам, клиентам конкурентам и должностным лицам окажутся беспочвенными.

Требования по защите коммерческой тайны могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор

заключается в устной форме, то действует требование по защите коммерческой тайны, вытекающее из правил внутреннего трудового распорядка. Об осведомлении в содержании правил внутреннего трудового распорядка лица, с которым заключается трудовой договор, делается отметка при ознакомлении его с приказом о приеме на работу. Таким образом, это создает необходимый элемент включения данного лица в механизм обеспечения сохранности коммерческой тайны. Один экземпляр договора обязательно должен быть вручен поступающему на работу сотруднику.

Использование договоров о неразглашении коммерческой тайны не является самостоятельной мерой по ее защите. Это только предупреждение сотруднику, что в дело вступает система мероприятий по организационной и инженерно-технической защите коммерчески ценной информации.

3.2. Организационная защита

Организационная защита информации – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий.

По мнению зарубежных специалистов, организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, т.к. возможности несанкционированного использования сведений конфиденциального характера в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, небрежностью и халатностью пользователей или персонала системы защиты. Влияние этих аспектов практически невозможно исключить с помощью технических средств, программно-математических методов и физических мер защиты. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которая исключила бы или сводила к минимуму возможность возникновения опасности утечки информации.

К *организационным мероприятиям* можно отнести:

- мероприятия, осуществляющиеся при проектировании, строительстве и оборудовании служебных и производственных помещений, исключающих возможность тайного проникновения на территорию и в помещения;
- мероприятия для обеспечения удобства контроля прохода и перемещения людей, проезда транспортных средств;
- мероприятия по созданию отдельных производственных зон по типу конфиденциальности работ с самостоятельными системами допуска;
- мероприятия, осуществляющиеся при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты конфиденциальной информации и др.;
- организация надежного пропускного режима и контроля посетителей;

- организация надежной охраны помещений и территории.

Организационные мероприятия охватывают самые различные источники информации и всевозможные каналы ее утечки, на которые возможно воздействовать организационными и довольно часто организационно-техническими мерами.

Организационные мероприятия при работе с сотрудниками предприятия в общем плане включают в себя:

- беседы при приеме на работу. В результате беседы устанавливается целесообразность приема кандидата на соответствующую вакантную должность. При приеме на работу возможно заключение соглашения между предприятием и сотрудником о частной информации, которая является собственностью предприятия и которую новый служащий обязуется соблюдать;
- ознакомление с правилами и процедурами работы с конфиденциальной информацией на данном предприятии. В подтверждение требований о сохранении в тайне коммерчески ценной информации поступающий на работу сотрудник дает подписку о сохранении коммерческой тайны предприятия, в которой обязуется не раскрывать секреты предприятия;
- обучение сотрудников правилам и процедурам работы с конфиденциальной информацией. Обучение сотрудников предполагает не только приобретение и систематическое поддержание на высоком уровне производственных навыков, но и психологическое их воспитание в плане убежденности в необходимости выполнения требований производственной секретности, информационной безопасности, защиты интеллектуальной собственности и коммерческой тайны. Систематическое обучение способствует развитию функциональной грамотности и повышению уровня компетентности руководства и сотрудников в защите коммерческих интересов своего предприятия.

Организуя регулярное обучение сотрудников, необходимо учитывать, что:

- часто утечка информации происходит из-за невежества сотрудников в оценке важности той или иной информации для упрочения престижа и финансовой стабильности предприятия;
- процесс обучения персонала должен быть непрерывным, организованным, обеспеченным материально, не должен иметь форму редких, часто необязательных собраний;
- необходимо иметь специальную программу обучения.

В этом случае необходимо учитывать:

- что представляет собой технология обработки и содержание деловой информации;
- насколько серьезно ее необходимо защищать;
- какие конкретно обязательства по обеспечению безопасности информации должен нести каждый конкретный сотрудник на конкретном участке работы;
- какие меры ответственности действуют в рамках данной организации.

Беседы с увольняющимися сотрудниками имеют главной целью

предотвратить утечку информации или ее неправильное использование.

Одним из важных направлений организационных мероприятий является четкая организация системы делопроизводства и документооборота. Система делопроизводства способствует рационализации и унификации документальных процессов и обеспечивает порядок делопроизводства, порядок учета, обработки, хранения, контроля наличия, правильности исполнения документов и уничтожения.

При реализации системы особое внимание уделяется обеспечению безопасности документов и конфиденциальной информации, в том числе закрепленной на технических носителях.

Целью организационных мероприятий при эксплуатации различных технических средств являются:

- определить технические средства, которые могут быть каналами утечки конфиденциальной информации;
- обеспечить их защиту или исключить из практики работы;
- осуществлять периодический контроль надежности технических средств защиты информации.

Организационные мероприятия по защите предприятия предусматривают:

- обеспечение безопасности зданий и территории;
- обеспечение безопасности отдельных зон и конкретных помещений;
- организацию четкой системы контроля допуска и доступа на территорию (помещение) к определенной информации.

Организационная защита коммерческой тайны.

В соответствии с Федеральным законом РФ от 29 июля 2004 г. №98-ФЗ «О коммерческой тайне» под *коммерческой тайной* понимается конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ услуг или получить коммерческую выгоду. *Информация*, составляющая *коммерческую тайну*, – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

Исходя из такого подхода, очевидно, что коммерческую тайну могут составлять сведения, характеризующие довольно широкий круг вопросов деятельности предприятия, причем сведения, которые составляют коммерческую тайну, могут быть открытыми, несекретными.

Для их защиты на предприятии должен быть определен свой порядок защиты. Следует подчеркнуть, что под разглашением информации, составляющей коммерческую тайну, законодатель понимает действие или бездействие, в результате которых информация, составляющая коммерческую

тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Вместе с тем следует иметь в виду, что защита технических, технологических, проектных и конструкторских решений, изобретений и т.п., появившихся в результате проведения работ по созданию вооружения или военной техники или связанных с разработкой новых материалов, новой техники и технологии, имеющих существенное значение для обороны и безопасности страны и являющихся по своему существу секретными, обеспечивается в соответствии с законодательством по защите секретной информации.

План мероприятий по защите коммерческих секретов предприятия.

1. Определение целей плана по защите коммерческой тайны.

Ими могут быть:

- предотвращение кражи коммерческих секретов;
- предотвращение разглашения коммерческих секретов сотрудниками, в том числе утечки через технические каналы.

2. Анализ сведений, составляющих коммерческую тайну:

- определить, какие сведения предприятия (технологические и деловые) являются коммерческой тайной;
- установить места ее накопления и хранения;
- выявить потенциальные каналы утечки сведений;
- оценить возможности предприятия по перекрытию этих каналов;
- проанализировать соотношение затрат и доходов по использованию различных технологий, обеспечивающих защиту коммерческой тайны;
- назначить сотрудников, ответственных за каждый участок системы обеспечения безопасности.

3. Обеспечить реализацию деятельности системы по следующим направлениям:

- контроль сооружений и оборудования предприятия (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль посещения предприятия и т.п.);
- работа с персоналом предприятия, в том числе проведение бесед при приеме на работу, инструктаж вновь принятых на работу по правилам и процедурам защиты информации, составляющей тайну предприятия; обучение сотрудников правилам сохранения коммерческих секретов; стимулирование сохранения конфиденциальности, беседы с увольняющимися;
- организация работы с конфиденциальными документами (установление порядка и правил ведения конфиденциального делопроизводства, контроль над конфиденциальными документами, контроль над публикациями; контроль и учет технических носителей конфиденциальных сведений, рассекречивание и уничтожение конфиденциальных документов, охрана чужих секретов);
- работа с конфиденциальной информацией, циркулирующей в

технических средствах и системах обеспечения производственной и трудовой деятельности (создание системы защиты конфиденциальной информации через технические каналы утечки);

- работа с конфиденциальной информацией, накопленной в компьютерных системах (создание системы защиты электронной информации от несанкционированного доступа к ней, обеспечение контроля за использованием технических средств).

3.3. Инженерно-техническая защита

В настоящее время на вооружении экономических разведок находятся самые разнообразные средства проникновения на объекты криминальных интересов и получения различными способами конфиденциальной информации, разработанные на основе последних достижений науки и техники, с использованием новейших технологий в области миниатюризации в интересах скрытого их использования против конкурентов. Противодействуя промышленному шпионажу, службы безопасности оснащаются необходимой им аппаратурой, не уступающей по надежности и функциональным возможностям аппаратуре разведки.

Инженерно-техническая защита – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности коммерческого предприятия. По функциональному назначению инженерно-техническая защита использует следующие средства:

- *физические средства защиты.* Они включают различные инженерные средства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных воздействий;
- *аппаратные средства защиты.* К данной категории относятся приборы, устройства, приспособления и другие технические решения, используемые в интересах обеспечения безопасности предприятия. В практике деятельности предприятий находит широкое применение самая различная аппаратура от телефонных аппаратов до совершенных автоматизированных информационных систем, обеспечивающих его производственную деятельность.
- *программные средства защиты.* Это специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
- *криптографические средства защиты* специальные математические и алгоритмические средства защиты информации, передаваемой по сетям связи, хранимой и обрабатываемой с использованием методов шифрования.

Такое деление средств достаточно условно, т.к. на практике довольно часто они взаимодействуют и реализуются в комплексе.

3.4. Универсальные меры обеспечения безопасности предприятия

Универсальные меры обеспечения безопасности предприятия – способы защиты, которые самостоятельно или в совокупности со средствами обеспечивают один или насколько видов защиты.

Выделяют следующие универсальные меры обеспечения информации:

1. Регламентация. Состоит в том, что все защитные мероприятия должны быть подчинены строго установленным правилам, закрепленным в нормативной базе.

2. Скрытие. Состоит в том, чтобы сделать незаметным сам факт существования защищаемого объекта или проведение любых работ по его защите.

3. Маркировка. Состоит в том, чтобы скрыть истинное состояние деятельности объекта.

4. Дезинформация. Состоит в том, чтобы подать заведомо ложную, но весьма правдоподобную информацию об объекте защиты.

5. Дробление (расчленение). Состоит в том, чтобы разнести части защищаемого объекта и хранить их независимо друг от друга.

6. Препятствие. Состоит в том, чтобы создать полосы препятствий на пути проникновения злоумышленника к защищаемому объекту.

4. ОРГАНИЗАЦИЯ СЛУЖБЫ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

4.1. Цели, задачи, функции службы безопасности
4.2. Структура службы безопасности

4.1. Цели, задачи, функции службы безопасности

Многогранность сферы обеспечения безопасности и защиты информационных ресурсов требует создания специальной службы, осуществляющей реализацию всех защитных мероприятий.

Служба безопасности (СБ) является важным структурным подразделением, организуемым администрацией предприятия для обеспечения целостности технико-технологических, экономических, правовых, коммерческих, режимных и физических компонентов предприятия, организации, учреждения.

Она формируется на основе анализа, оценки и прогнозов их внутренней деятельности, с целью решения задач защиты интересов предприятия, организации, учреждения.

Ее статус определяется соответствующим приказом руководителя предприятия либо решением вышестоящей организации, в которую оно входит.

Служба безопасности является структурной единицей предприятия, непосредственно участвующей в его работе. Структура и штаты СБ

определяются руководителем предприятия в зависимости от объема работ и особенностей производственно-коммерческой деятельности. Назначение на должность начальника СБ предприятия, а также его освобождение производится только руководителем предприятия.

Правовое оформление СБ проходит через регистрацию в органах государственной безопасности и внутренних дел, но подчиняется только руководителю предприятия, учреждения, организации либо одному из заместителей, которому поручено непосредственно ее курировать, чаще всего это лицо, занимающееся вопросами режима.

Основные положения, состав и организация СБ имеют юридическую силу в том случае, если они зафиксированы в основополагающих правовых, юридических и организационных документах предприятия.

Соотношение угроз экономической безопасности предприятия с анализом реальной обстановки на предприятии, отношений с партнерами, поставщиками и клиентами, особенностей конкуренции позволит выявить задачи, которые должна решать СБ предприятия для достижения этой цели.

Решение о формировании СБ принимается на основе разработанных документов (устава предприятия), в которых сформированы цели, задачи и обязанности этой службы.

Целью деятельности СБ является своевременное выявление и нейтрализация причин и условий, способствующих утечке информации, составляющей коммерческую тайну, нанесению материального и морального ущерба предприятию.

Основными *задачами СБ* являются:

1. Обеспечение производственно-торговой деятельности, защиты информации и сведений, являющихся коммерческой тайной.
2. Организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческих секретов.
3. Организация специального делопроизводства, исключающего несанкционированное получение сведений, составляющих коммерческую тайну.
4. Предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим тайну предприятия.
5. Выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной деятельности и в экстремальных ситуациях.
6. Обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, связанные с деловым сотрудничеством, как на национальном, так и на международном уровне.
7. Обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности.
8. Обеспечение безопасности персонала предприятия, в том числе

разработка мер обеспечения физической защиты персонала, организация охраны, пропускного, внутриобъектового режима, обеспечение персонала средствами технической защиты от несанкционированного проникновения в помещения, автомашины, квартиру, на стоянку, правовое обучение персонала.

9. Оценка маркетинговых исследований и неправомерных действий конкурентов и злоумышленников.

В своей деятельности СБ руководствуется:

1. Инструкцией по организации режима и охране.
2. Инструкцией по обеспечению безопасности сведений, составляющих коммерческую тайну.
3. Перечнем сведений, составляющих коммерческую тайну.
4. Инструкцией по работе с конфиденциальной информацией для руководителей, специалистов и технического персонала.
5. Инструкцией по организации хранения дел, содержащих конфиденциальную информацию.
6. Инструкцией по организации инженерно-технической защиты информации.
7. Инструкцией о порядке работы с иностранными представителями и представительствами.

Для решения основных задач, поставленных перед СБ, она должна выполнять различные *функции,* которые наиболее адекватно соответствуют производственно коммерческой деятельности предприятия.

- *Административно-распорядительная* – реализуется путем участия СБ в подготовке решений по установлению и поддержанию системы безопасности, определению полномочий, прав, обязанностей и ответственности должностных лиц по вопросам обеспечения безопасности объекта.
- *Хозяйственно-распорядительная* – предусматривает участие СБ в определении ресурсов, необходимых для решения задач безопасности объекта, в подготовке и проведении мероприятий по обеспечению сохранности имущества, финансов, интеллектуальной и иной собственности.
- *Социально-кадровая* - реализуется участием СБ в подборе и расстановке кадров, выявлении возможных причин и условий возможных конфликтов, а также их локализации; создании нормальной обстановки; инструктаже персонала по вопросам своей компетенции; контроле за соблюдением правил режима и безопасности.
- *Социально-управленческая* – заключается в участии СБ в создании и поддержании организационной структуры управления процессом обеспечения безопасности, а также гибких временных структур по отдельным направлениям работы; в организации взаимодействия и координации между отдельными звеньями системы для достижения поставленных целей.
- *Планово-производственная* – реализуется в разработке комплексной программы и отдельных подсистемных целевых планов обеспечения безопасности объекта; в подготовке и проведении мероприятий по их осуществлению и поддержке режима безопасности.

▪ *Организационно-техническая* – осуществляется путем материально-технического и финансового обеспечения системы безопасности объекта, подготовки и проведения мероприятий по их осуществлению; освоения специальной техники (в том числе освоения новых видов техники для специальной деятельности).

▪ *Научно-методическая* – реализуется в накоплении и освоении опыта обеспечения безопасности; организации обучения сотрудников предприятия; научном анализе возникающих проблем обеспечения безопасности и методическом сопровождении деятельности предприятия в этой сфере.

▪ *Информационно-аналитическая* – заключается в целенаправленном сборе и обработке информации, относящейся к сфере безопасности; в создании и использовании необходимых технических и методических средств аналитической обработки информации; в организации информационного обеспечения заинтересованных подразделений и отдельных лиц в сведениях, имеющихся в службе безопасности.

▪ *Учетно-контрольная* – реализуется работой по организации своевременного обнаружения внешних и внутренних угроз финансовой стабильности и устойчивости предприятия, оценкой их источников, налаживанием контроля за критическими ситуациями, ведением учета негативных факторов, влияющих на безопасность предприятия.

4.2. Структура службы безопасности

Деятельность СБ заключается в создании необходимых правовых, организационных и материальных условий выявления, предупреждения и пресечения посягательств криминальных структур на имущество, интеллектуальную собственность, благоприятную финансово-коммерческую конъюнктуру, устойчивость хозяйственных связей, социально-психологическую обстановку, производственную дисциплину.

Создание СБ требует тщательного учета и анализа индивидуальных особенностей предприятия: его размеров, численности персонала, структуры, используемых технологий, производственных схем, действующих связей, особенностей циркуляции информации.

При создании службы безопасности необходимо:

1. Определить соотношение тех составляющих СБ, которые будут выполнять специфические функции по обеспечению безопасности (охрана объектов), и тех, которые должны управлять процессом обеспечения функционирования других подразделений предприятия с точки зрения безопасности. Структура и состав этих подразделений СБ в значительной степени будут определяться размерами предприятия.

2. При определении структуры службы безопасности необходимо исходить из соотношения затраты-эффективность, имея в виду возможность в определенной степени использовать услуги имеющихся специализированных предприятий.

Возможно, при такой организации работы какому-то предприятию достаточно привлечь специалиста по вопросам обеспечения безопасности.

Практически на всех предприятиях существуют структурные подразделения (юридическое, экономического анализа и маркетинга), отвечающие за подбор кадров, охрану труда и технику безопасности, осуществляющие охрану материальных ценностей, пропускной режим. Для крупных предприятий, имеющих многочисленный персонал, высокорентабельное производство, целесообразно создание полномасштабной структуры службы безопасности, включающей в себя несколько подразделений, которые своей деятельностью обеспечивают решение задач по четырем направлениям:

1. Охрана материальных ценностей.
2. Защита коммерчески ценной информации.
3. Работа по персоналу.
4. Обеспечение безопасности коммерческой деятельности.

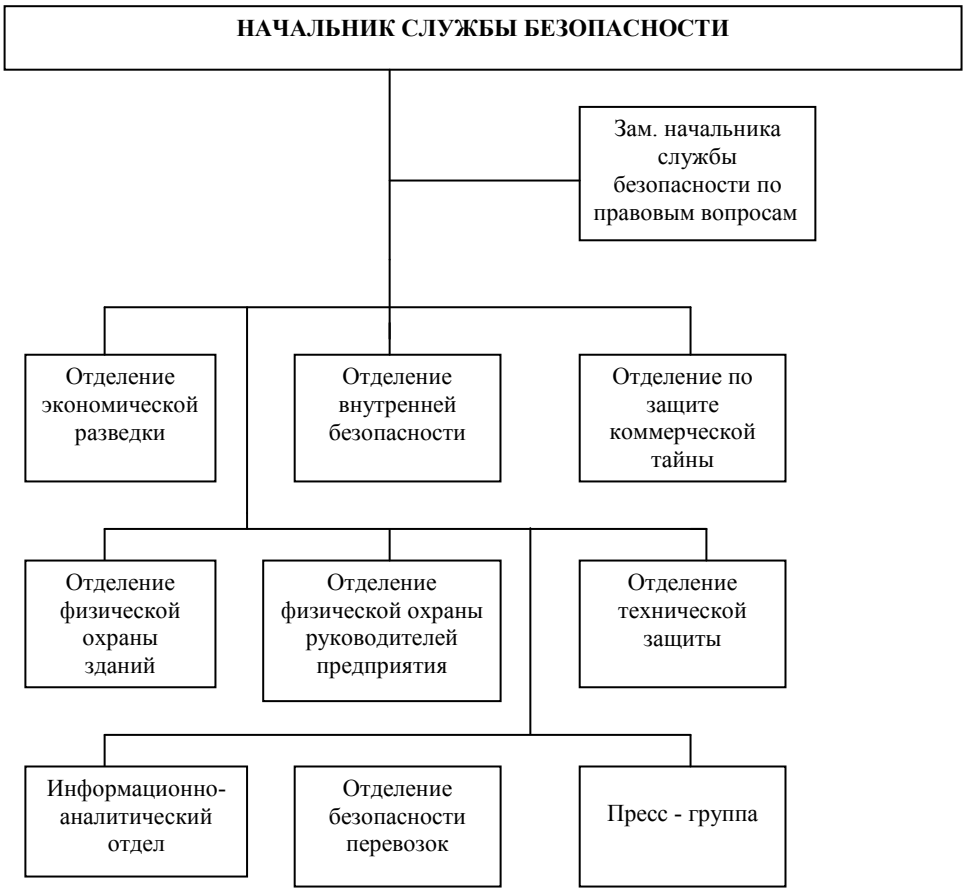

Рис. 4.1. Структура службы безопасности предприятия

При создании СБ целесообразно пользоваться консультациями специалистов – бывших сотрудников правоохранительных органов или специальных служб, т.к. деятельность службы безопасности во многом должна строиться на принципах работы этих учреждений.

Структура службы безопасности и ее штаты определяются в соответствии

с целями, функциями и задачами обеспечения безопасности предприятия. Ее деятельность должна быть направлена на комплексное решение поставленных задач на основе разработанной стратегии и применения взаимосвязанных тактических приемов подготовки и проведения мероприятий по обеспечению безопасности.

Взаимоотношения СБ со службами и подразделениями предприятия определяются уставом и организационно-распорядительными документами по вопросам этих отношений, которые оформляются соответствующими приказами и распоряжениями руководителей предприятия.

Ответственность СБ перед руководителями предприятия, его структурными подразделениями и трудовыми коллективами определяется в соответствии с ее функциями. За результаты своей работы она и ее сотрудники несут юридическую, материальную и дисциплинарную ответственность

ГЛАВА 5. ОРГАНИЗАЦИЯ РЕЖИМА И ОХРАНЫ

5.1. Основные задачи режима и охраны
5.2. Требования внутриобъектового режима
5.3. Организация пропускного режима
5.4. Виды пропусков

5.1. Основные задачи режима и охраны

Основной задачей службы безопасности по *обеспечению режима и охраны* является организация и осуществление мер по обеспечению безопасности деятельности и защите информации предприятия всеми возможными в конкретных условиях способами и средствами.

В целях обеспечения надежной охраны материальных ценностей, конфиденциальных документов и информации, содержащей сведения конфиденциального характера, а также своевременного предупреждения попыток несанкционированного доступа к ним устанавливается определенный режим деятельности, соблюдение которого обязательно для всех сотрудников, посетителей и клиентов.

Режим – это система ограничительных мероприятий, правил и норм, обеспечивающих контролируемый доступ или допуск на определенную территорию, в помещение, к информации и документам.

Режим и охрана – это сочетание организационных, регламентационных и контрольных мер, направленных на обеспечение полной (круглосуточной, в течение длительного времени), частичной (только в ночное или в дневное время), выборочной (при завозе ценных грузов, на определенный отрезок времени и т.п.) сохранности физических лиц, материальных и финансовых ценностей, зданий и помещений предприятия, а также любых сведений о деятельности предприятия, не подлежащих разглашению. Соблюдение этих мер обязательно для всех сотрудников, посетителей и клиентов.

Руководители и сотрудники предприятия, обеспечивающие и осуществляющие режим и охрану, руководствуются в своей деятельности соответствующим законодательством и нормативными документами.

Цель создания режима и охраны определяет его задачи, выбор способов, а также сил и средств для охраны.

Задачи подразделяются на *основные* и *обеспечивающие*.

К основным задачам относятся:

1. обеспечение сохранности зданий и помещений предприятия;
2. сохранность и контроль за перемещением товарно-материальных ценностей;
3. обеспечение пропускного режима (или контроль за допуском граждан в здания и помещения);
4. сохранность собственной информации о деятельности предприятия;
5. поддержание противопожарной безопасности.

В число обеспечивающих задач входят:

1. подбор, подготовка сил и средств;
2. контроль функционирования системы режима и охраны;
3. материально-техническое обеспечение режима и охраны;
4. сбор и анализ информации о состоянии режима.

Принципами режима и охраны являются:

1. целесообразность;
2. активность;
3. рациональное использование сил и средств;
4. скрытность;
5. стремление к максимальной информированности.

Эффективный режим охраны призван обеспечить сохранность зданий и помещений на объекте, сохранность и контроль за перемещением товарно-материальных ценностей и людей, предупредить утечку информации о деятельности объекта, поддерживать противопожарную безопасность. Решающее значение для режима охраны имеют квалифицированный подбор, подготовка и расстановка сил и средств охраны, а также контроль функционирования службы безопасности на объекте.

Основными *принципами* режима и охраны являются:

1. активность и предупредительный характер охраны, что заключается в опережающем выявлении признаков готовящейся атаки объекта и своевременном принятии мер по ее предупреждению или пресечению (отражению);
2. целесообразность и обоснованность организации режима охраны объекта, своевременность его усиления, рациональное использование сил и средств охраны;
3. разумное сочетание собственных возможностей и возможностей сил правоохранительных органов для обеспечения безопасности объекта;
4. осуществление охраны по единому плану;
5. скрытность или демонстративность охраны в зависимости от ситуации,

складывающейся вокруг охраняемого объекта;

6. максимальная информированность охраны обо всех событиях, происходящих на объекте.

Задачи режима охраны. В практике деятельности подразделений охраны по обеспечению безопасности выделяют две группы задач режима охраны объекта:

1. аналитические и предупредительные;

2. процедурно-отражательные.

Аналитические задачи решаются путем систематического сбора информации об объектах преступной деятельности и состоянии собственного режима охраны. Главным здесь является соблюдение принципов непрерывности и постоянства сбора информации.

Решение предупредительных задач связано в первую очередь с созданием имиджа сильного и надежного режима охраны.

Вторая группа задач режима охраны объекта решается путем своевременного обнаружения признаков готовящегося посягательства с последующим его отражением предварительно подготовленными силами и средствами.

Особое внимание деятельности охранников следует уделять при решении задач обеспечения поведения на охраняемом объекте деловых встреч и приемов партнеров по бизнесу. В этом плане служба охраны должна обеспечить:

1. встречу гостей, прибывших на деловой прием;
2. согласование действий основной охраны и телохранителей приглашенных лиц;
3. охрану одежды, вещей гостей и их автомобилей на прилегающей территории;
4. предупреждение инцидентов между гостями на деловом приеме или встрече;
5. выявление участников, которые ведут себя необычно, и др.

5.2. Требования внутриобъектового режима

Внутриобъектовый режим – это установленный на предприятии порядок выполнения правил внутреннего трудового распорядка, направленных на обеспечение экономической безопасности, сохранения материальных средств и защиты конфиденциальной информации.

Внутриобъектовый режим предусматривает следующие:

- установление четкого распорядка рабочего времени;
- строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности;
- установление порядка приема и работы с посетителями сторонних организаций;
- оборудование предприятия техническими средствами обеспечения

производственной деятельности (связь, автоматизация, охранная и пожарная сигнализация, замки, ограждения и др.);

- порядок сдачи и приема помещений под охрану;
- порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности и экономии.

Работа с представителями сторонних организаций осуществляется в следующем порядке:

- принимающий специалист накануне делает заявку канцелярии на следующий день с указанием Ф.И.О. прибывающих, их места работы и предполагаемого времени прибытия;
- в день прибытия канцелярия фиксирует их прибытие в журнале учета посетителей и приглашает специалиста фирмы;
- специалист встречает прибывших, получает в канцелярии ключи от комнаты переговоров и сопровождает туда посетителей. Запрещается прием посетителей сторонних организаций в других помещениях фирмы без специального на то разрешения директора или его заместителя;
- в ходе работы необходимо плотно закрывать окна и шторы;
- по окончании работы с посетителями принимающий специалист провожает их до выхода из офиса и делает в журнале учета посетителей соответствующие отметки о времени их ухода. Во время пребывания посетителей принимающий специалист обязан контролировать их пребывание и действия. После завершения встречи специалист закрывает комнату переговоров и сдает ключи от нее в канцелярию.

5.3. Организация пропускного режима

Цели, задачи и требования к контрольно-пропускному режиму.

Построение надежной системы безопасности предприятия – сложный и многогранный процесс. Одним из немаловажных факторов обеспечения надежной защиты того или иного объекта является организация и поддержание определенного *контрольно-пропускного режима*.

Контрольно-пропускной режим является неотъемлемой частью общей системы безопасности предприятия. Контрольно-пропускной режим (как и вся система безопасности) должен соответствовать действующему законодательству, уставу предприятия, а также нормативно-правовым актам, регулирующим деятельность предприятия.

Контрольно-пропускной режим – это система организационно-правовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты, в отдельные здания (помещения) сотрудников объекта, посетителей, транспорта и товарно-материальных ценностей.

Создание надежного контрольно-пропускного режима требует значительных затрат. Однако если внимательно оценить все негативные факторы, воздействующие на деятельность предприятия (фирмы), эти затраты

не окажутся столь большими, т.к. обеспечивается устойчивое экономическое положение предприятия (фирмы) и сводятся к минимуму возможные потери. К тому же процесс создания системы контрольно-пропускного режима может быть растянут во времени, с учетом материальных возможностей предприятия (фирмы) и условий его деятельности на рынке. Принципиально важным условием для реализации замысла является анализ ситуации и разработка программы действий, что позволит избежать излишних затрат.

Основные *цели контрольно-пропускного режима* сводятся к следующему:

1. защита законных интересов и прав предприятия, поддержание устойчивого порядка внутреннего управления;
2. сохранение собственности предприятия, ее рационального и эффективного использования;
3. способствование росту прибылей предприятия;
4. достижение внутренней и внешней стабильности предприятия;
5. сохранение коммерческих секретов и прав на интеллектуальную собственность.

Для достижения целей контрольно-пропускного режима он должен отвечать следующим требованиям:

- обеспечение санкционированного прохода сотрудников и посетителей, ввоза (вывоза) продукции и материальных ценностей, ритмичной работы предприятия;
- исключение незаконного прохода лиц на охраняемые территории и в отдельные здания (помещения), бесконтрольного въезда (выезда) транспортных средств;
- своевременное выявление угроз жизненно важным интересам предприятия, причин и условий, способствующих нанесению предприятию материального и морального ущерба, его нормальному функционированию и развитию;
- формирование надежных гарантий поддержания организационной стабильности внешних и внутренних связей предприятия, отработка механизма оперативного реагирования на угрозы и негативные тенденции в развитии;
- пресечение посягательств на законные интересы предприятия, использование юридических, экономических, организационных, социально-психологических, технических и иных средств выявления и ослабления источников угрозы.

Требования к контрольно-пропускному режиму должны быть доведены в обязательном порядке до каждого сотрудника объекта под роспись. Все рабочие и служащие объекта обязаны соблюдать их. По каждому случаю нарушения контрольно-пропускного режима должна проводиться служебная проверка.

Обязанность охраны по контрольно-пропускному режиму определяется в инструкции и должностных обязанностях контролеров контрольно-пропускных пунктов.

Разработка инструкции о пропускном режиме.

Пропускной режим является неотъемлемой частью общей системы охраны предприятия. Практическое решение этих вопросов оформляется в виде «Инструкции о пропускном режиме». Указанная инструкция должна определять систему организационно-охранных мер, устанавливающих разрешительный порядок (режим) прохода (проезда) на объект (с объекта) и может включать:

1. Общие положения. В этом разделе указываются:

- нормативные документы, на основании которых составлялась инструкция;
- определение контрольно-пропускного режима и цель его установления;
- на кого возлагается руководство пропускным режимом и практическое его осуществление;
- санкции к нарушителям контрольно-пропускного режима;
- требования к оборудованию различных помещений.

2. Порядок пропуска сотрудников предприятия, командированных лиц и посетителей через контрольно-пропускные пункты. В этом разделе рекомендуется:

- перечислить все КПП и их назначение, описание, расположение и установить их единую нумерацию;
- изложить требования к оборудованию КПП;
- установить порядок прохода сотрудников и посетителей на территорию объекта и в категорированные подразделения;
- определить права и основные обязанности контролеров КПП;
- установить помещения, где запрещается принимать посетителей и представителей сторонних организаций.

3. Порядок допуска на объект транспортных средств, вывоза (выноса) продукции, документов и материальных ценностей. В этом разделе указывается:

- порядок допуска на территорию объекта (с объекта) автотранспорта, принадлежащего объекту;
- въезд и стоянка на территории объекта транспорта, принадлежащего сотрудникам на правах личной собственности;
- порядок пропуска автотранспорта сторонних организаций, прибывших с грузом в адрес объекта в рабочее и нерабочее время;
- порядок ввоза (вывоза) материальных ценностей;
- правила оформления документов на вывоз (вынос) материальных ценностей с территории объекта.

4. Виды пропусков, порядок их оформления. В этом разделе определяется:

- виды пропусков, их количество и статус;
- описание пропусков;
- порядок оформления и выдачи пропусков;
- общая замена и перерегистрация пропусков;
- мероприятия при утере пропуска сотрудником.

5. Обязанности должностных лиц по поддержанию контрольно-пропускного режима.

6. Учет и отчетность, порядок хранения пропусков и печатей.

В зависимости от структуры предприятия и характера его деятельности инструкция может содержать и другие разделы.

5.4. Виды пропусков

Для пропуска на предприятие, в отдельные помещения, как правило, устанавливается несколько видов пропусков, дающих право прохода сотрудников и посетителей на предприятие, вноса (выноса) ввоза (вывоза) материальных ценностей. Это могут быть: *постоянные, временные, разовые и материальные пропуска, удостоверения.* Образцы бланков пропусков или удостоверений разрабатываются администрацией предприятия (службой безопасности). По своему внешнему виду и содержанию пропуска должны отличаться друг от друга и обладать защитными свойствами. Все виды пропусков, за исключением материальных, оформляются и выдаются бюро пропусков (или иным подразделением) по письменным заявкам. Виды пропусков или удостоверений определяются в зависимости от специфики предприятия.

На пропусках и удостоверениях проставляются печати, предусмотренные правилами режима, и цифровые знаки, определяющие зону доступности, период их действия, право проноса портфелей (кейсов, папок др.). Период пребывания сотрудников на предприятии в рабочее и нерабочее время определяется руководством с проставлением цифр знака на пропуске или удостоверении. Утвержденные образцы удостоверений личности, пропусков, оттисков цифровых знаков, печатей (штампов), проставляемых на пропусках или удостоверениях с образцами подписей руководителей или уполномоченных лиц, имеющих право подписывать пропуска или удостоверения, передаются начальнику отдела режима и охраны под расписку.

Полная замена постоянных пропусков или удостоверений осуществляется, как правило, через 3-5 лет. Через 2-3 года производится их перерегистрация с проставлением соответствующей отметки.

Для перерегистрации, замены или изменения пропускных документов ежегодно по состоянию на 1 января в службу безопасности представляются кадровой службой списки сотрудников с указанием должности, фамилии, имени, отчества и наименование документа с соответствующими пометками (круглосуточно, рабочее время с _____ по _____, с портфелем, в какую зону и т.п.).

Удостоверения и постоянные пропуска выдаются сотрудникам объекта, принятым на постоянную работу, а также работникам других организаций, закрепленным для постоянного обслуживания объекта. Удостоверения и постоянные пропуска выдаются лицам, не работающим на данном предприятии, по отдельному утвержденному руководством списку с указанием

учреждения, должности, фамилии, имени, отчества и сопроводительных пометок. Эти документы должны постоянно храниться в бюро пропусков (или у уполномоченного лица) и выдаваться посетителю в момент его прибытия. После завершения работы эти лица сдают документы в бюро пропусков.

Временные пропуска с фотографиями на срок до трех месяцев выдаются лицам, работающим временно, или прикомандированным. Временные пропуска без фотографии на срок до одного месяца действуют при предъявлении паспорта (удостоверения личности) предъявителя. Продление действия временных пропусков допускается на срок не более двух месяцев.

Разовые пропуска (для посетителей и клиентов) выдаются на одно лицо и только для разового посещения предприятия и его структурных подразделений. Пропуск оформляется и действителен при наличии документа, удостоверяющего личность. Разовые пропуска должны периодически меняться по цвету бланков и другим отличительным признакам.

Разовый пропуск, выданный водителю транспортного средства, может служить одновременно разовым пропуском для транспорта.

Разовый пропуск изымается на посту контролером при выходе посетителя из предприятия и сдается в бюро пропусков. О лицах, не покинувших предприятие по истечении установленного срока действия пропуска, контролер докладывает начальнику караула (дежурному по КПП) для принятия мер по выяснению причин задержки. Фамилии лиц, посетивших предприятие по разовому пропуску, могут записываться в специальный журнал (книгу) учета.

Материальные пропуска для вывоза (выноса) товарно-материальных ценностей выдаются администрацией предприятия. Срок действия пропуска определяется инструкцией о контрольно-пропускном режиме. Материальные пропуска должны изыматься на КПП и сдаваться в бюро пропусков.

ГЛАВА 6. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ТРАНСПОРТИРУЕМЫХ ГРУЗОВ ПРЕДПРИЯТИЯ

6.1. Общие положения перевозки грузов различными транспортными средствами

6.2. Организация охраны грузов на железнодорожном транспорте

6.3. Организация охраны грузов, перевозимых автомобильным транспортом

6.4. Охрана грузов при использовании воздушного транспорта

6.1. Общие положения перевозки грузов различными транспортными средствами

Важнейшее условие договора перевозки, заключаемого между транспортными структурами и грузоотправителями, – обеспечение сохранности перевозимых грузов. Борьба с потерями грузов при перевозке имеет, помимо юридического, первостепенное экономическое значение.

Ответственность транспортных организаций за сохранность перевозимых грузов возникает с момента приема их к перевозкам и прекращается в момент выдачи получателю. К потерям грузов при перевозке можно отнести – хищения, недостачи массы или мест, утрату, порчу или повреждение груза. Согласно Уставам, которыми руководствуются транспортные ведомства, они обязаны возместить грузополучателю причиненные убытки.

Однако материальная ответственность может быть возложена на транспортные организации лишь в том случае, если потеря произошла по их вине, а доказать это по многим причинам грузоотправителю удается не всегда. Поэтому предприниматель, связавший себя с государственными и негосударственными транспортными структурами, может оказаться в невыгодной для себя ситуации.

По усмотрению предпринимателя его грузы могут перевозиться эшелонами, отдельными вагонами в составе эшелона, в специальных вагонах, крытых вагонах (полувагонах, на платформах) в составе грузовых поездов, в почтово-багажных вагонах пассажирских поездов, в отдельных купе пассажирских вагонов, самолетами (вертолетами), автомобилями, водным транспортом, а также смешанным способом.

Охрана грузов является выполнением договорных требований предпринимателей и требует от сотрудников охраны точного соблюдения всех положений контракта, надежности и инициативы. Виновные в нарушении требований контракта должны нести административную, материальную и уголовную ответственность.

В целях выполнения требований договора составу охраны необходимо:

1. Обеспечить надежную охрану груза независимо от его количества.

2. Сохранять в тайне от окружающих характер груза, пункт его отправления и назначения с целью сохранения коммерческой тайны и во избежание ее утечки к преступным лицам.

3. Задерживать лиц, пытающихся посягать на охраняемый груз, и отражать возможные нападения.

Сотрудник охраны или группа охранников приступает к выполнению своих обязанностей после распоряжения руководителя предприятия или лица, его замещающего, согласно заключенному договору.

Маршруты для транспортировки охраняемых грузов целесообразно по расстоянию разделять на:

1. Местные (в пределах города, населенного пункта);

2. Дальние (при перевозках за пределы города, населенного пункта, региона).

Охрану грузов целесообразно организовать таким образом, чтобы она как можно меньше привлекала внимание.

Предприниматель, организующий охрану груза, должен учитывать:

- Условия договора по охране груза.
- Предполагаемую нагрузку на каждого сотрудника охраны.
- Особенности конкретных маршрутов.

- Характер возможных действий криминальных структур.
- Вероятностные изменения в организации охраны по ходу маршрута.

Предприниматель должен совершенствовать организацию охраны и ее материально-техническую базу и обеспечение, контролировать специальную и физическую подготовку персонала.

Знание особенностей маршрутов, по которым транспортируются грузы, может существенно помочь предпринимателю более квалифицированно осуществлять подбор и подготовку персонала охраны, проверять качество охраны в пути следования.

Перед принятием решения по комплектованию групп охраны предпринимателю необходимо выслушать мнение психолога (если он имеется) о психологической совместимости членов группы. В каждой группе охраны независимо от ее численного состава назначается *старший*. Подбор старших групп целесообразно осуществлять с учетом их деловых и моральных качеств, способности выполнять требуемый объем работ, самостоятельно принимать решения в случае изменения обстановки, организовывать работу подчиненных, заставить их выполнять требования дисциплины и субординации.

Принимая решение по комплектованию групп, предприниматель должен учитывать:

1. Состав группы.
2. Характер перевозимого груза.
3. Продолжительность несения службы в темное и светлое время суток.
4. Время прибытия группы к грузоотправителю.

Численность охраны зависит от материальных возможностей предпринимателя, который заказывает или организует охрану грузов. Ориентировочно эта численность может быть:

1. При охране от 1 до 7 вагонов – 3 человека.
2. При охране от 8 до 14 вагонов – 6 человек.
3. При охране свыше 14 вагонов – до 15 человек.
4. Для охраны груза, перевозимого в самолете или купе поезда, – 2-3 человека.
5. Для охраны груза, перевозимого в автомобиле, сроком до суток, – 2-3 человека, при перевозке свыше суток – 4 человека.
6. При охране груза, перевозимого колонной автомобилей, – 1 охранник на каждый автомобиль и 2-3 резервных, следующих в автомобиле без груза.

В зависимости от ценности (важности) груза, характера и продолжительности охраны, численность охраны может быть увеличена по усмотрению как самого заказчика охраны, так и предпринимателя, выделяющего охрану.

6.2. Организация охраны грузов на железнодорожном транспорте

При перевозке грузов железнодорожным транспортом группа охраны прибывает к грузоотправителю не позже чем за один час до приема груза, при

этом старший группы предъявляет отправителю удостоверение старшего группы, проверяет у представителя заказчика документы, уточняет количество и тип вагонов, время готовности и порядок приема транспорта под охрану.

Перед началом поездки старший группы должен проверить:

- исправность и оборудование вагона-помещения для охраны (обеспеченность топливом, освещением на весь путь следования);
- исправность вагонов (крыш, полов, стен, надежность крепления дверей, дверных накладок, люков), бортов на полувагонах и платформах;
- правильность наложения закруток на дверных накладках, правильность пломбирования вагонов (четкость оттисков на пломбах при сличении их с имеющимися образцами);
- число вагонов, полувагонов, платформ;
- число мест в полувагонах и на платформах, прочность крепления, исправность упаковки.

В случае обнаружения неисправностей или неполного оборудования вагона для размещения охраны старший группы имеет право приостановить прием транспорта (груза) и потребовать от представителя заказчика устранения выявленных недостатков.

В пути следования старшему группы рекомендуется:

- в зависимости от времени года через каждые 2-4 часа производить смену охраны и производить осмотр груза;
- осмотр вагонов (груза, упаковок, пломб, печатей) на стоянках при смене поездных бригад или если продолжительность стоянки поезда более 10 минут;
- на остановках усиливать охрану за счет свободных охранников.

По прибытии в пункт назначения старший группы сдает груз получателю, при этом он сообщает о прибытии груза заказчику через начальника станции или дежурного по станции; проверяет у грузополучателя документы на право приема грузов или транспорта с грузом и документы, удостоверяющие его личность. При охране груза, транспортируемого в отдельном вагоне (купейном, плацкартном, почтово-багажном), желательно присутствие заказчика.

При транспортировке груза в купе пассажирского поезда его охрана осуществляется силами 2-3 человек, руководствуются следующими правилами:

- купе должно быть закуплено полностью, т.е. посторонних в нем не должно быть;
- проверить, чтобы в купе не было посторонних предметов;
- проверить исправность запоров на дверях и окнах;
- двери в купе закрываются, ставятся на предохранительную защелку на весь путь следования;
- охраняемый груз должен располагаться только на нижней полке – так, чтобы он все время находился в поле зрения охраны и одновременно исключалась возможность его падения, порчи.

Охране запрещается:

- оставлять купе без присмотра даже на время;

- в случае острой необходимости оставлять купе по очереди;
- допускать в купе посторонних лиц;
- хранить охраняемый груз на багажной полке, на полу, в ящике под нижней полкой, т.к. в этом случае не исключено его хищение из соседнего купе;
- пользоваться для приема пищи вагоном-рестораном.

При возникновении пожара, аварии в купе или вагоне охрана принимает участие в ликвидации происшествия, не ослабляя надежности охраны груза. Если происшествие угрожает безопасности груза, принять меры к его выносу в безопасное место.

При перевалке груза с автомобиля в вагон старший группы следует за несущим груз, а охранник – впереди него. Груз несет представитель заказчика. Старший группы проверяет, чтобы в автомобиле, доставившем груз к поезду, не осталось частей груза. Это вызвано тем, что места наибольшего скопления людей – криминогенные зоны, в которых наиболее велика вероятность различных нежелательных ситуаций. В присутствии заказчика или его представителя проверяется исправность упаковки груза. При обнаружении недостатков представитель заказчика их устраняет. Если с грузом следует представитель заказчика, он имеет право располагаться в купе вместе с охраной.

6.3. Организация охраны грузов, перевозимых автомобильным транспортом

Вся охрана, следующая в автотранспорте, обязана уметь водить как минимум те марки автомобилей, на которых они охраняют груз. Если перевозка осуществляется одним автомобилем, один охранник располагается в кабине, второй (старший группы) – в левом переднем углу кузова (ближе к водителю).

Перед началом поездки старший группы охраны обязан:

- в присутствии представителя заказчика проверить исправность и надежность крепления бортов автомобиля, количество мест (контейнеров) в кузове, исправность упаковки и надежность крепления груза;
- при погрузке, вскрытии и выгрузке груза не допускать к автомобилю посторонних лиц;
- в случае открывания бортов автомобиля, угрозы падения груза и других неисправностей принять меры к остановке автомобиля и устранению неисправностей;
- при поломке автомобиля в пути следования организовать перегрузку груза своими силами, не ослабляя надежности охраны;
- при аварии автомобиля и разбросе груза принять меры к его сбору и усилению охраны;
- если при аварии произошел несчастный случай, допускать к автомобилю только сотрудников милиции и медицинских работников.

На стоянке старший группы располагается впереди автомобиля слева, охранник – сзади справа.

6.4. Охрана грузов при использовании воздушного транспорта

Для перевозки груза в самолете (вертолете) выделяется группа охраны, состоящая из 2-3 человек. При перегрузке груза из автомобиля в самолет (вертолет) целесообразно одного охранника оставлять на автомобиле до полной выгрузки, а старшему группы следовать с первой партией груза в самолет (вертолет) и находиться там до прибытия охранника с последней партией груза, обращая внимание на число охраняемых мест и недопустимость повреждения упаковки. При размещении груза в транспортном самолете или салоне пассажирского самолета старший группы выставляет охранника около груза, в багажном отсеке пассажирского самолета – у люка (в этом случае охранник при посадке должен входить последним, а выходить первым).

В случае перевозки груза в салоне пассажирского самолета, в силу специфики расположения пассажирских мест, груз должен быть компактным и надежно замыкаться. Как правило, это портфели, небольшие саквояжи, которые в аэропортах пересадок переносятся прикрепленными к запястью охранника. Самыми безопасными в случае захвата самолета террористами являются места в среднем салоне возле окон – обычно террористы располагаются в первом салоне, ближе к пилотской кабине, а также в последних рядах хвостового салона. Опыт показывает, что люди, сидящие на местах у проходов, чаще оказываются жертвами применения оружия как со стороны преступников, так и со стороны группы захвата. Учитывая, что при захвате самолетов террористы не преследуют целей ограбления, группе охраны целесообразно запретить вступать в бой ни при захвате самолета террористами, ни при штурме самолета группой захвата.

ГЛАВА 7. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Основные направления компьютерных преступлений
7.2. Классификация компьютерных преступлений
7.3. Защита компьютерных данных

Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего, компьютерных сетей. Это дает основание поставить задачу компьютерного права, одним из основных аспектов которого являются так называемые компьютерные посягательства.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное

обеспечение и базы данных, для которых технические средства являются окружением.

На сегодняшний день сформулированы базовые *принципы информационной безопасности,* которая должна обеспечивать:

• *целостность данных* – защиту от сбоев, ведущих к потере информации, а также от неавторизованного создания или уничтожения данных.

• *конфиденциальность информации* и одновременно ее доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надежности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

7.1. Основные направления компьютерных преступлений

Компьютерные преступления – это предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть. Компьютерные преступления условно можно подразделить на две большие категории:

• преступления, связанные с вмешательством в работу компьютеров;

• преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

1. Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакер, «компьютерный пират» – лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе и путем распространения компьютерных вирусов). С одной стороны, «хакер» – это человек, который прекрасно знает компьютер и пишет хорошие программы, а с другой – незаконно проникающий в компьютерные системы с целью получения информации.

Английский глагол «to hack» применительно к компьютерам может означать две вещи – взломать систему или починить ее. В основе этих действий

лежит: понимание того, как устроен компьютер, и программы, которые на нем работают.

Таким образом, слово «хакер» совмещает в себе, по крайней мере, два значения: одно – окрашенное негативно («взломщик»), другое – нейтральное или даже хвалебное («ас», «мастер»). Другими словами, хакеров можно разделить на «плохих» и «хороших».

«Хорошие хакеры» двигают технический прогресс и используют свои знания и умения на благо человечества. Ими разработано большое число новых технических и программных систем.

Им, как водится, противостоят «плохие» – они читают чужие письма, воруют чужие программы и всеми доступными способами вредят прогрессивному человечеству.

«Плохих хакеров» можно условно разделить на четыре группы. *Первая, состоящая в основном из молодежи, – люди, взламывающие компьютерные системы просто ради собственного удовольствия.* Они не наносят вреда, а такое занятие весьма полезно для них самих – со временем из них получаются превосходные компьютерные специалисты.

Вторая группа – пираты. Они взламывают защиту компьютеров для похищения новых программ и другой информации.

Третья группа – хакеры, использующие свои познания действительно во вред всем и каждому. Они уничтожают компьютерные системы, в которые им удалось прорваться, читают чужие письма, а потом издеваются над их авторами.

Есть и еще одна группа – *хакеры, которые охотятся за секретной информацией по чьим-либо заказам.*

Среди российского хакерства выделяются четыре основных типа.

Первый – романтики-одиночки. Они, как правило, взламывают базы данных из чистого любопытства. В целом они довольно безопасны и бескорыстны, но и наиболее талантливы. Поэтому массовые взломы компьютерных сетей какой-либо фирмы обычно начинаются после того, как на нее набредет кто-то из "романтиков" и похвастается этим в своей сети.

Второй – прагматики или классики. Работают как в одиночку, так и группами. Воруют, как говорится, что придется: игры, программы, электронные версии разных изданий. Например, еще в сентябре 1995 фирма "Майкрософт" с большой помпой представляла в Москве "WINDOWS95". По оценкам западной прессы, на рекламу нового продукта ушло около 300 миллионов долларов. И «фирмачи» потом долго не могли понять, почему в России эта новейшая база раскупается так плохо. А дело в том, что наши хакеры еще в апреле взломали главный компьютер "Майкрософта", украли оттуда засекреченный тогда "WINDOWS" и наладили продажу его по ценам, дешевле фирменных.

Третий – разведчики. Сегодня в любой уважающей себя фирме имеется хакер, оформленный обычно как программист. Его задача – взламывать сети конкурентов и красть оттуда самую разную информацию. Этот тип пользуется сейчас наибольшим спросом.

Четвертый – кибергангстеры. Это уже профессиональные компьютерные бандиты, работают они в основном на мафиозные структуры. Их задачи конкретные: блокировка и развал работы компьютерных сетей разных "неугодных" российских и западных фирм, а также кража денег с банковских счетов. Дело это дорогое и небезопасное, зато самое высокооплачиваемое.

Следующие преступления, связанные с вмешательством в работу компьютера:

2. Ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

"Временная бомба" – разновидность "логической бомбы", которая срабатывает по достижении определенного момента времени.

3. Способ "троянский конь" состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью "троянского коня" преступники, например, отчисляют на свой счет определенную сумму с каждой операции.

4. Разработка и распространение компьютерных вирусов.

5. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти недостижима.

6. Подделка компьютерной информации.

По-видимому, этот вид компьютерной преступности является одним из наиболее «свежих». Он является разновидностью несанкционированного доступа, с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосовании, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

7. Хищение компьютерной информации.

Если "обычные" хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется

как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является “средством” достижения цели.

1. Разработка сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными – рекомендации по выбору оптимального варианта действий преступника.

2. Преступления с общим названием – “воздушный змей”.

В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз (“воздушный змей” поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно “перескакивает” с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

7.2. Классификация компьютерных преступлений

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран.

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного. Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений:

QAH – "Компьютерный абордаж" (хакинг – hacking): доступ в компьютер

или сеть без права на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

QAI – перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

- *"Жучок"* (bugging) – характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;

- *"Откачивание данных"* (data leakage) – отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;

- *"Уборка мусора"* (scavening) – характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности – физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;

- метод следования *"За глупцом"* (piggbackiiig), характеризующий несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;

- метод *"За хвост"* (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;

- метод *"Неспешного выбора"* (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;

- метод *"Поиск бреши"* (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

- метод *"Люк"* (trapdoor), являющийся развитием предыдущего. В найденной "бреши" программа "разрывается", и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу;

- метод *"Маскарад"* (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;

- метод *"Мистификация"*(spoofing), который используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты**.**

Изменение компьютерных данных (QD) включает в себя следующие виды преступлений:

QDL/QDT – логическая бомба (logic bomb), троянский конь (trojan horse): изменение компьютерных данных без права на то, путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь – заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

QDV – вирус (virus): изменение компьютерных данных или программ, без права на то, путем внедрения или распространения компьютерного вируса.

Компьютерный вирус – это специально написанная программа, которая может "приписать" себя к другим программам (т.е. "заражать" их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

QDW - червь: изменение компьютерных данных или программ, без права на то, путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способы совершения компьютерных преступлений:

QFC – компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

QFF – компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

QFG – мошенничества и хищения, связанные с игровыми автоматами.

QFM – манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается *метод подмены данных кода* (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

QFP – компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

QFT – телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлений:

QRG/QRS – незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

QRT – незаконное копирование топографии полупроводниковых изделий: копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

Компьютерный саботаж (QS) составляют следующие виды преступлений:

QSH – саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

QSS – компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

К прочим видам компьютерных преступлений (QZ) в классификаторе отнесены следующие:

QZB – использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности;

QZE – хищение информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну, без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества;

QZS – использование компьютерных систем или сетей для хранения,

обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия.

- *"Временная бомба"* – разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;

- *"Асинхронная атака"* (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей.

- *"Моделирование"* (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления.

7.3. Защита компьютерных данных

Защита данных, защита информации [data protection] – совокупность мер, обеспечивающих защиту прав собственности владельцев информационной продукции, в первую очередь – программ, баз и банков данных от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме.

Уже в первых публикациях по защите информации были изложены основные постулаты, которые не утратили своей актуальности и по сей день.

Первый постулат гласит*: абсолютно надежную, непреодолимую защиту создать нельзя*. Система защиты информации может быть в лучшем случае адекватна потенциальным угрозам. Поэтому при планировании защиты необходимо представлять, кого и какая именно информация может интересовать, какова ее ценность для вас и на какие финансовые жертвы ради нее способен пойти злоумышленник.

Из первого постулата вытекает второй: *система защиты информации должна быть комплексной, т.е. использующей не только технические средства защиты, но и административные и правовые.*

Третий постулат состоит в том, что *система защиты информации должна быть гибкой и адаптируемой к изменяющимся условиям*. Главную роль в этом играют административные (или организационные) мероприятия, – такие, например, как регулярная смена паролей и ключей, строгий порядок их хранения, анализ журналов регистрации события в системе, правильное распределение полномочий пользователей и многое другое. Человек, отвечающий за все эти действия, должен быть не только преданным сотрудником, но и высококвалифицированным специалистом как в области технических средств защиты, так и в области вычислительных средств вообще.

Сегодня известно много мер, направленных на предупреждение преступления. Выделим из них три: *технические*, *правовые* и *организационные*.

К техническим мерам можно отнести:

• защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем;

• организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев;

• установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды;

• принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов;

• установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К правовым мерам следует отнести:

• разработку норм, устанавливающих ответственность за компьютерные преступления;

• защиту авторских прав программистов;

• совершенствование уголовного и гражданского законодательства, а также судопроизводства.

К организационным мерам относят:

• охрану вычислительного центра;

• тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком;

• наличие плана восстановления работоспособности центра после выхода его из строя;

• организацию обслуживания вычислительного центра посторонней организацией или лицами, не заинтересованными в сокрытии фактов нарушения работы центра;

• универсальность средств защиты от всех пользователей (включая высшее руководство);

• возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

Методы физической защиты данных.

При рассмотрении проблем защиты данных прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных.

Одним из эффективных способов сохранения конфиденциальности информации является ее *кодирование (шифрование)*. Делается это с помощью специальных криптографических программ, которые кодируют и/или декодируют содержимое файлов с применением шифра.

Однако подвергать шифрованию абсолютно всю информацию – дело весьма трудоемкое и дорогостоящее. В основном в зашифрованном виде производится хранение информации – шифруются архивы, базы данных. Но при работе с информационными хранилищами на определенном этапе происходит дешифрация данных и ее передача в открытом виде. В этот момент возможные сбои вычислительных систем чреваты серьезными последствиями.

Рассмотрим наиболее уязвимые места вычислительных систем.

Кабельная система остается главной “ахиллесовой пятой” большинства локальных вычислительных сетей: по данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети.

Наилучшим является использование так называемых структурированных кабельных систем, это означает, что кабельную систему можно разделить на несколько уровней в зависимости от назначения и месторасположения компонентов кабельной системы.

Системы электроснабжения. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания. Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельной компьютера в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитных носителях. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства – серверы, концентраторы, мосты и т.д. – оснащены собственными дублированными системами электропитания.

Системы архивирования и дублирования информации. Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер. Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

Защита от стихийных бедствий. Основной и наиболее распространенный метод защиты информации и оборудования от различных стихийных бедствий - пожаров, землетрясений, наводнений и т.д. – состоит в хранении архивных копий информации или в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях или, реже, даже в другом районе города или в другом городе.

На сегодня защита данных обеспечивается законодательными актами на международном и государственном уровне. В России такими законодательными актами служат закон "Об информации, информатизации и защите информации" (базовый) и закон "О правовой охране программ для электронных вычислительных машин и баз данных".

В настоящее время некоторые статьи УК РФ также направлены на защиту информации.

ГЛАВА 8. БИЗНЕС - РАЗВЕДКА

8.1. Роль разведки в обеспечении экономической безопасности предприятия
8.2. Информационные потребности предприятия
8.3. Разведка конкурентов
8.4. Планирование разведывательной деятельности
8.5. Виды и методы разведки
8.6. Принципы и технология добывания информации
8.7. Определение эффективности добывания информации

8.1. Роль разведки в обеспечении экономической безопасности предприятия

Для успешной деятельности на рынке любому предприятию необходима полная и достоверная информация о потребителях, фирмах-партнерах, конкурентах, о выпускаемой в отрасли продукции, товарных рынках, рынке ценных бумаг, инвестиционных возможностях и т.д. То есть нужна деловая информация.

Особую важность деловая информация имеет для предприятий, планирующих выпуск новых товаров или выход на новые рынки. В этом случае речь идет о получении сведений о потенциальных партнерах и потребителях. Эту задачу решают службы безопасности предприятий, ориентированные на разведывательную деятельность.

По неофициальным оценкам сотрудников ФСБ России, практически каждая крупная отечественная фирма крадет информацию у своих конкурентов и одновременно страдает от аналогичных действий с их стороны. Опыт последних лет показывает, что прочность положения предприятия в значительной степени зависит от владения информацией о рыночной конъюнктуре, финансовом положении конкурентов, результатах перспективных исследований и разработок, тенденциях развития в конкретных областях бизнеса, получить которую должна экономическая разведка.

Разведка является широкой и многогранной сферой деятельности, прямо или косвенно она связана почти со всеми отраслями знаний.

Необходима система сбора, обработки, анализа информации, ее хранения и использования, классификация признаков готовящихся преступлений по всем указанным проблемам, этапы их подготовки, систематизация этих признаков и разработка на их основе системы прогнозов возможных подрывных или иных акций. Для этого необходима разработка источников информации, средств, форм и методов ее получения, не запрещенных законодательством России.

Определение *конкурентной разведки* можно дать через ее главную задачу – поддержку оптимальных решений по управлению путем обеспечения информацией, основанной на результатах деятельности по сбору и аналитической обработке данных о внешней среде, в которой действует эта

структурная единица.

Термины «информация» и «аналитическая обработка данных» указывают на то, что для принятия оптимальных решений требуются не отрывочные исходные данные, а тщательно взвешенная, проверенная, обобщенная и убедительно представленная информация.

По мнению отечественных и зарубежных специалистов, имеется ряд некоторых важнейших задач, к решению которых целесообразно привлечь службу коммерческой разведки (КР):

- поиск путей развития, позволяющих предприятию получить существенные преимущества над своими конкурентами;
- разработка принципиально новых подходов к ведению бизнеса, открывающих предприятию пути к захвату лидерства в отрасли;
- своевременное раскрытие планов конкурентов по достижению конкурентного преимущества, захвата лидерства или совершению иных принципиально опасных для предприятия действий.

8.2. Информационные потребности предприятия

Информационная потребность является одним из центральных понятий предпринимательства. Когда поставлена цель и сформулирована задача, возникает необходимость в информации.

Информационная потребность определяется по-разному: как информация, необходимая для достижения какой-либо цели, или свойство отдельного лица, коллектива или какой-либо системы, отображающее необходимость получения информации, соответствующей характеру выполняемых действий или работ.

При самом общем решении проблемы информационной потребности необходимо иметь в виду три компонента:

1. Человека (потребителя информации), который формулирует свои задачи.
2. Фонд информации (информационный массив), в котором сосредоточена необходимая информация.
3. Соответствующее устройство, которое является посредником между потребителем информации и информационным массивом. Это устройство называется информационной системой.

Информационный массив необходимо организовать, т.е. информация в нем должна быть упорядочена таким образом, чтобы при запросах потребителю выдавалась лишь та информация, которая ему необходима. Следовательно, информационная система должна быть в состоянии определить, что же должен потребитель получить в действительности, объективно, а не исходить из того, что он субъективно полагает необходимым узнать.

Как правило, изучение информационных потребностей происходит в форме естественного эксперимента, происходящего при непосредственных контактах специалиста по разведке с заказчиком. Это легкий, но ненадежный

путь. Он не дает достаточной картины того, что необходимо заказчику на самом деле.

Руководитель предприятия как заказчик информации должен назвать конкретные параметры, которые ему необходимо знать и по которым он должен принять решение о дальнейшем сотрудничестве с конкретным предприятием.

Следует отметить, что изучение информационных потребностей – это постоянное уточнение интересов заказчика. Уточнение может осуществляться в результате текущих, рабочих обсуждений проблемы с заказчиком, анализа реакции заказчика на предоставленную ему информацию, изучения документальных материалов на основе последних научных достижений.

Информацию принято считать ценной лишь тогда, когда ее можно использовать, причем полезность информации во многом зависит от ее полноты, точности и своевременности.

Следует различать и не путать факты (данные), мнения (личностные предложения) и информацию (аналитически обработанные данные). При этом следует отличать так называемые *информационные шумы*, вводящие в заблуждение и отвлекающие внимание от основного вопроса.

Осознав, что информация необходима, нужно прояснить следующие вопросы:

- Что нужно узнать?
- Где (и в каком виде) может быть желаемая информация?
- Кто ее может знать или достать?
- Как (и в каком виде) ее можно получить?

Четкие ответы на начальные вопросы обеспечивают понимание последнего, техника решения которого зависит как от существующих внешних условий, так и от знаний, воли, опыта, возможностей и изобретательности.

Получив исходную информацию, ее необходимо:

- оценить (по степени достоверности, важности, секретности, возможности использования);
- интерпретировать (в свете других данных и интуиции), выявив ее место в общей мозаике фактов;
- определить, необходима ли дополнительная (и какая) информация;
- эффективно использовать (учесть в своих планах, передать, кому это необходимо, придержать до нужного момента и т.д.).

8.3. Разведка конкурентов

Разведка конкурентов может включать тайные операции по сбору финансовых и внутрикорпоративных сведений, данных о производстве, технических и научных сведений, информации о маркетинге и юридических сведений. Ее цели:

1. Получать своевременную точную и подробную информацию о

возможностях и путях выбора у основных конкурентов.

2. Определить пути, которыми основные конкуренты могут нанести ущерб текущим интересам данной организации.

3. Постоянно наблюдать и получать достоверную и полную информацию относительно ситуации и соприкосновения интересов в конкурентных и смежных областях на рынке, которые могли бы повлиять на интересы данной организации.

4. Накапливать полную и достоверную информацию относительно политической, экономической, юридической, социальной и технологической систем, затрагивающих конкурентные возможности данной организации.

5. Добиться эффективности и устранить дублирование усилий в сборе, анализе и сортировке разведывательных данных всей организации.

Теоретически этих целей можно добиться, не прибегая к неэтическим или незаконным методам. В действительности, многие корпорации создали разветвленные системы сбора разведывательных данных о конкурентах, которые основаны целиком на открытых источниках: это данные о продажах; сведения казначейства; научных и исследовательских учреждений; отраслевая литература; профессиональные ассоциации; покупатели; распространители и поставщики; местные торговые палаты; пресса; ежегодные отчеты; собрания держателей акций; инвестиционные банки; торговые отделы; высший управленческий состав; соглашения о лицензиях и т.д. Однако эти открытые источники не могут обеспечить конкурентного преимущества. Кроме того, развитие технологий происходит настолько быстро, что отраслевая литература за ними не успевает. Искушение прибегнуть к промышленному шпионажу настолько велико, что многие безупречные во всех других отношениях компании создали специальные подразделения для проведения промышленного шпионажа.

Основными задачами и соответствующими им направлениями разведывательной деятельности являются:

- определение цели проведения разведывательной деятельности;
- изучение информационных потребностей руководства и специалистов предприятия;
- определение источников информации;
- подготовка информационно-аналитических документов для заказчика и/или специалистов предприятия;
- учет результатов разведывательной деятельности;
- определение эффективности разведывательной деятельности.

Под термином *система коммерческой разведки (СКР)* понимается организационная структура, занимающаяся вопросами добывания, сбора, проверки (верификации), обработки и анализа данных по различным аспектам экономической деятельности предприятия, его партнеров с дальнейшим использованием полученной информации для решения конкретных задач его хозяйственной деятельности.

Основное назначение СКР – в обеспечении руководства достоверной,

объективной и полной информацией о намерениях партнеров, смежников, клиентов и контрагентов, о сильных и слабых сторонах конкурентов; сборе данных, позволяющих оказывать влияние на позицию оппонентов в ходе деловых переговоров, оповещении о возможном возникновении кризисных ситуаций; мониторинге и контроле хода реализации заключенных договоров и достигнутых ранее договоренностей.

При рассмотрении возможной модели реализации СКР на предприятии следует учитывать, что масштабы и количество привлекаемых на ее создание и эксплуатацию средств во многом определяются возможностями самого предприятия и рамками стоящих перед ним задач.

Исходя из вышеизложенного, можно определить цели разведки в предпринимательской деятельности:

1. Своевременное обеспечение руководителей предприятия надежной и всесторонней информацией об окружающей предприятие среде. Выявление факторов риска, которые могут затронуть экономические интересы предприятия и помешать его нормальному функционированию.

2. Организация максимально эффективной информационной работы, исключающей дублирование структурными подразделениями предприятия друг друга.

3. Выработка краткосрочных и долгосрочных прогнозов влияния окружающей среды на хозяйственную деятельность предприятия. Разработка рекомендаций по локализации и нейтрализации факторов риска.

4. Установление благоприятных и локализация неблагоприятных факторов влияния окружающей среды на хозяйственную деятельность предприятия.

Цель коммерческой разведки может быть сформулирована и иным образом, но в любом случае она должна отражать следующие моменты:

1. Своевременность выявления и предоставления потребителю (руководству предприятия) необходимой информации (очевидно, что при отсутствии или запаздывании соответствующей информации невозможно принять меры по ликвидации и нейтрализации угрозы деятельности предприятия).

2. Необходимо поставлять потребителю только качественную информацию. Такой она будет только в том случае, если установлены:

а) *важность* (способность внести вклад в деятельность предприятия);

б) *точность* (надежность источника и самой информации);

в) *значимость* (ценность и правильное понимание информации).

3. Сфера действия коммерческой разведки должна находиться во внешней среде функционирования предприятия. Именно внешняя среда функционирования является объектом разведывательной деятельности предприятия. Она включает:

1) поставщиков (юридические и физические лица, обеспечивающие предприятие и его конкурентов материальными ресурсами, необходимыми для производства конкретных товаров или услуг);

2) маркетинговых посредников (фирмы, помогающие предприятию в

продвижении, сбыте и распространении его товаров), включающих:

- торговых посредников (деловые фирмы, помогающие предприятию подыскивать клиентов и/или непосредственно продавать им товары);
- фирмы по организации товародвижения (склады, транспортные предприятия и т.д.);
- агентства по оказанию маркетинговых услуг;
- кредитно-финансовые учреждения (банки, кредитные страховые компании и т.д.).

3) клиентуру;

4) конкурентов;

5) контактные аудитории (любая группа, которая проявляет реальный или потенциальный интерес к предприятию или оказывает влияние на его способность достигать поставленных целей.

Организационная структура СКР включает два вида подразделений: *добывающие и информационные*. Основное назначение добывающих подразделений состоит в добывании всеми доступными и не противоречащими законодательству средствами и методами сведений, документов, предметов и других материалов, которые представляют или могут представлять разведывательный интерес. На финансирование добывающих подразделений приходится 80% затрат всей разведки. Добывающие подразделения должны быть ориентированы на сбор, накопление, хранение, поиск, переработку информации и выдачу ее пользователям.

Основная задача информационных подразделений разведки состоит в оценке, классификации, анализе и предоставлении руководству предприятия обработанной разведывательной информации. В состав этих подразделений входят аналитическое отделение, отделение стратегического планирования, справочно-информационный фонд, группа экспертов и консультантов.

Между всеми подразделениями СКР должно быть четкое разграничение функций, задач и форм представления результатов работы.

8.4. Планирование разведывательной деятельности

Принято выделять следующие основные принципы планирования разведывательной деятельности:

1. Определение потребности субъекта предпринимательской деятельности в информации для достижения свих целей.
2. Определения цели разведывательной деятельности.
3. Определение источников получения необходимой информации.

Для продуктивного ведения хозяйственной деятельности руководству предприятия требуется принимать разноуровневые решения, информационную поддержку которых обеспечивает СКР.

Управление любой организацией включает, как минимум, два уровня: управление текущей деятельностью предприятия и его стратегическим развитием.

Необходимо отметить, что характер информации для каждого уровня принимаемых решений будет различным.

В связи с этим работу подразделения коммерческой разведки целесообразно разделить на две составляющие.

Стратегическая составляющая разведки – сбор и анализ стратегической информации о глобальных процессах в экономике, политике, технологии и т.д., которые могут оказать влияние (положительное или негативное) на развитие предприятия.

Цель стратегического решения (открытие нового производства, внедрение на рынок нового товара или услуг и т.п.) заключается в определении направления дальнейшего развития предприятия. Эти решения определяют потребность сориентироваться на рынке и проанализировать перспективы его развития.

Оперативно-тактическая (микроэкономическая) составляющая разведки – сбор и анализ оперативно-тактической информации для принятия руководством обоснованных решений по текущим проблемам предприятия.

Цель оперативно-тактического решения (строительство или приобретение здания под новый цех, обучение персонала для выпуска новой продукции или оказания новой услуги) при определенной стратегии дальнейшего развития – выбрать оптимальный путь его достижения и минимизировать затраты.

Цели разведывательной деятельности жестко структурированы. Каждая цель предопределяется целью высшего порядка, оставаясь при этом автономной по характеру своих потребностей и источников информации.

8.5. Виды и методы разведки

В настоящее время разведку условно можно разделить на *агентурную и техническую*. Условность состоит в том, что добывание информации агентурными методами зачастую осуществляется с использованием технических средств, а техническую разведку ведут люди. Отличия – в преобладании человеческого или технического фактора.

Агентурная разведка – наиболее древний и традиционный вид разведки. Добывание информации проводится агентом-разведчиком путем проникновения к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее потребителю.

Развитие технической разведки связано, прежде всего, с повышением ее технических возможностей, обеспечивающих:

- снижение риска физического задержания агента органами контрразведки или службы безопасности за счет дистанционного контакта его с источником информации;
- добывание информации путем съема ее с носителей, не воздействующих на органы чувств человека.

Многообразие видов носителей информации породило множество видов

технической разведки. Ее классифицируют по различным признакам (основаниям классификации). Наиболее широко применяются две классификации: по физической природе носителя информации и видам технических средств добывания.

Техническая разведка (при классификации по физической природе носителя информации) состоит из следующих видов:

- оптическая (носитель – электромагнитное поле в видимости и инфракрасном диапазоне);
- радиоэлектронная (носитель – электромагнитное поле);
- акустическая (носитель – акустическая волна);
- химическая (носитель – частицы вещества);
- радиационная (носитель – излучения радиоактивных веществ);
- магнитометрическая (носитель – магнитное поле).

В свою очередь, оптическая, радиоэлектронная и акустическая разведка подразделяется на подвиды:

Оптическая разведка включает:

- визуально-оптическую;
- фотографическую;
- инфракрасную;
- телевизионную;
- лазерную.

Радиоэлектронная разведка (РЭР) классифицируется по нескольким признакам:

- целевое назначение;
- место базирования (местонахождение) средств разведки;
- характер добываемой информации;
- используемые принципы и средства разведки.

РЭР в зависимости от характера добываемой информации подразделяется на:

- радиоразведку;
- радиотехническую;
- радиолокационную;
- радиотепловую.

Помимо основных видов необходимо также выделить основные *методы разведки*.

Для добывания и сбора разведывательных данных используются самые разнообразные методы. Многие из них не отличаются особой порядочностью, однако они являются неизменно эффективными:

- закупка товаров конкурентов;
- присутствие на ярмарках, выставках, конференциях и т.п. При этом собирается вся доступная или оставленная по недосмотру документация и информация, фотографируется все, что возможно;
- посещение предприятий;

- финансирование контрактов на выполнение научно-исследовательских работ за рубежом с целью проникновения в некоторые лаборатории;
- отправка на учебу за рубеж студентов и стажеров;
- длительные безрезультатные переговоры, в процессе которых постоянно запрашивается дополнительная информация;
- похищение чертежей и технической документации;
- шпионаж;
- внедрение своего сотрудника на конкурирующее предприятие, в качестве сотрудника (метод «засланного казачка»).

8.6. Принципы и технология добывания информации

Основными принципами добывания информации являются целеустремленность, активность, непрерывность, скрытость, комплексное использование сил и средств.

Целеустремленность предусматривает определение задач и объектов разведки, ведение ее по единому плану и сосредоточение усилий органов разведки на выполнение основных задач.

Активность предполагает активные действия всех элементов СКР по добыванию информации, прежде всего по поиску оригинальных способов и путей решения задач применительно к конкретным условиям.

Непрерывность разведки подчеркивает постоянный характер добывания информации и независимость этих действий от времени года, суток, погоды, любых условий обстановки. При изменении обстановки в соответствии с принципом активности меняются способы и средства добывания.

Скрытность ведения разведки обеспечивается путем проведения мероприятий по подготовке и добыванию информации в тайне, в интересах как безопасности органов добывания, так и скрытия фактов утечки или изменения информации. Реализация этого принципа позволяет разведке повысить безопасность органа добывания и выиграть время для более эффективного применения добытой информации.

О том, что конфиденциальная информация стала достоянием конкурента, руководство предприятия узнает обычно по ряду косвенных признаков:

- снижению доходов или усилению позиций конкурента в связи с выбросом на рынок аналогичных товаров, но с лучшими потребительскими свойствами или по более низким ценам;
- появлению публикаций в периодической печати и патентов по результатам исследований, ведущихся в лабораториях фирмы;
- перераспределению традиционной клиентуры в пользу конкурента.

Эффективность добывания информации достигается путем комплексного использования различных способов и средств разведки, что обеспечивает дублирование данных по основным направлениям и приводит к повышению достоверности получаемой информации.

Добывание информации на основе указанных принципов осуществляется постоянно легальными способами и при недостаточности полученной этими способами информации – путем тайных операций.

Легальное добывание информации проводится путем изучения и обработки по интересующим разведку вопросам публикаций в СМИ, периодических научных и популярных журналах, Интернет – ресурсах, трудах высших учебных заведений и научно-производственных организаций, правительственных изданиях, учебных пособиях и др.

Ценную информацию можно получить из правительственных источников, отчетов фирм по операциям с ценными бумагами, из судебных материалов, освещающих ход судебного разбирательства с участием конкурентов, и из других источников.

Необходимую информацию можно найти в материалах, имеющих непосредственное отношение к деятельности фирмы: в лицензиях, статьях и докладах, годовых отчетах фирм, обзорах рынков и докладов консультантов, внутренних печатных изданиях, телефонных справочниках, рекламной литературе и проспектах и др.

Однако *наиболее ценная информация добывается нелегальным путем*, в результате проведения тайных мероприятий органами коммерческой разведки.

Технология добывания информации предусматривает следующие этапы:

- организация добывания;
- добывание данных и сведений;
- информационная работа.

Организация добывания информации включает:

- декомпозицию (структурирование) задач, поставленных пользователями информации;
- разработку замысла операции по добыванию информации;
- планирование;
- постановку задач исполнителям;
- нормативное и оперативное управление действиями исполнителей и режимами работы технических средств.

На результативность добывания информации влияют многочисленные факторы – противодействие контрразведки и службы безопасности, недостаточность информации об источниках добываемых сведений и данных, отказы аппаратуры, погодные условия и др. Эти факторы учитываются при планировании и постановке задач с указанием места и времени действия всех исполнителей и технических средств, участвующих в операции по добыванию информации.

Методы доступа к информации.

Методы доступа к информации можно разделить на три группы:

- физическое проникновение к источнику информации;
- сотрудничество органа разведки с работником конкурента, имеющего легальный или нелегальный доступ к интересующей информации;
- дистанционный съем информации с носителя или источника.

Физическое проникновение к источнику информации возможно путем скрытого или с применением силы проникновения злоумышленника к месту хранения носителя, а также в результате внедрения злоумышленника в организацию. Способ проникновения зависит от вида информации и способов ее использования.

Скрытое проникновение имеет ряд преимуществ по сравнению с остальными, но требует тщательной подготовки и априорной информации о месте нахождения источника, системе безопасности, возможных маршрутах движения и др. Кроме того, скрытое проникновение не может носить регулярный характер, т.к. оно связано с большим риском для злоумышленника и приемлемо для добывания чрезвычайно ценной информации.

Для обеспечения регулярного доступа к информации проводится внедрение и легализация сотрудника СКР путем его поступления на работу в интересующую организацию.

Приведенные выше способы обеспечивают скрытность добывания информации. Когда в ней нет необходимости, а цена информации очень высока, то возможно нападение на сотрудников охраны с целью похищения источника информации. К таким источникам относятся, например, документы, которыми можно шантажировать конкурента или вытеснить его с рынка после опубликования.

Основными способами привлечения таких сотрудников являются инициативное сотрудничество и склонение к сотрудничеству.

Инициативное сотрудничество предполагает привлечение людей, которые ищут контакты с разведкой конкурента, к сотрудничеству с ним с целью добывания секретной или конфиденциальной информации по месту работы. В основе инициативного сотрудничества в подавляющем большинстве случаев лежат корыстные и аморальные мотивы, которые часто прикрываются рассуждениями о высоких целях.

Способы склонения к сотрудничеству подбираются под конкретного человека, который попал в поле зрения органов разведки и которого предполагается заставить сотрудничать. Наиболее распространенным и менее опасным способом склонения к сотрудничеству является подкуп. Подкупленный сотрудник может стать постоянным и инициативным источником информации.

Другие способы склонения к сотрудничеству связаны с насильственными действиями злоумышленников. Это психологическое воздействие, угрозы личной безопасности, безопасности родственников, а также преследования и шантаж, принуждающие сотрудника фирмы нарушить свои обязательства о неразглашении тайны. Если в результате предварительного изучения личностных качеств сотрудника фирмы, его жизни и поведения выявляются компрометирующие данные, то возможен шантаж сотрудника с целью склонения его к сотрудничеству под угрозой разглашения компрометирующих сведений.

Выведывание – способ получения информации от человека путем

задавания ему вопросов. Способы выведывания весьма разнообразны – от срытого выведывания до пытки. Скрытое выведывание возможно путем задавания в ходе беседы на конференции, презентации и/или другом месте вроде бы невинных вопросов, ответы на которые для специалиста содержат конфиденциальную информацию. Применяется скрытое выведывание в устной или письменной форме при фиктивном найме на работу сотрудника конкурирующей фирмы на более высокооплачиваемую или интересную работу. После получения в беседе с претендентом нужной информации ему под различными предлогами отказывают в приеме на работу.

Дистанционное добывание информации предусматривает съем ее с носителей, распространяющихся за пределы помещения, здания, территории предприятия, организации. Она возможна в результате наблюдения, подслушивания, перехвата, сбора носителей информации в виде материальных тел за пределами предприятия.

Наблюдение предполагает получение и анализ изображения объекта наблюдения. При наблюдении добываются в основном видовые признаки объектов. Но возможно добывание семантической информации, если объект наблюдения представляет собой документ, схему, чертеж и т.д.

Объекты могут наблюдаться непосредственно или с помощью технических средств. Различают следующие способы наблюдения с использованием технических средств:

- визуально-оптическое;
- с помощью приборов наблюдения в ИК-диапазоне;
- наблюдение с консервацией изображения (фото и видеосъемка):
- телевизионное наблюдение, в том числе с записью изображения;
- радиолокационное наблюдение;
- радиотеплолокационное наблюдение.

Современный состав приборов визуально-оптического наблюдения довольно разнообразен – от специальных телескопов до эндоскопов. Т.к. человеческий глаз не чувствителен к ИК-лучам, то для наблюдения в ИК-диапазоне применяются специальные приборы (ночного видения, тепловизоры), преобразующие невидимое изображение в видимое.

Радиолокационное наблюдение позволяет получать изображение удаленного объекта в радиодиапазоне в любое время суток и в неблагоприятных климатических условиях, когда невозможны другие способы наблюдения. При радиотеплолокационном наблюдении изображение объекта соответствует распределению температуры на его поверхности.

Подслушивание, как и наблюдение, бывает непосредственным и с помощью технических средств. Непосредственное подслушивание использует только слуховой аппарат человека. В силу малой мощности речевых сигналов разговаривающих людей и значительного затухания акустической волны в среде распространения. Поэтому для подслушивания применяются различные технические средства.

Перехват предполагает несанкционированный прием радио- и

электросигналов и извлечение из них семантической информации.

Многообразие технических средств и их комплексное применение для добывания информации порой размывает границы между рассмотренными способами. Например, при перехвате радиосигналов сотовой системы телефонной связи возможно подслушивание ведущихся между абонентами разговоров – одновременно производится и перехват, и подслушивание. Учитывая неоднозначность понятий «подслушивание» и «перехват», способы добывания акустической информации целесообразно относить к подслушиванию, а несанкционированный прием радио- и электросигналов – к перехвату.

Добывание конфиденциальной информации без проникновения в контролируемую зону осуществляется путем съема информации с ее носителей, распространяющихся за пределы контролируемой зоны. Под контролируемой зоной понимается физическое ограждение или условно (в документах) обозначенная территория, в пределах которой обеспечивается защита информации или проводятся мероприятия по защите информации. Внешней границей контролируемой зоны является граница территории предприятия, организации или государственных структур.

За пределы территории возможен выход следующих носителей:

- людей;
- бумажных и машинных носителей с документами и публикациями, продукции, материалов, сырья, оборудования;
- акустических, электрических, магнитных и электромагнитных полей, телефонной сети, охранной и пожарной сигнализации и др.

Эти носители могут содержать семантическую и признаковую информацию.

8.7. Показатели эффективности добывания информации

Наиболее общим показателем эффективности разведки, включающей органы управления, добывания и обработки, является степень выполнения поставленных перед нею задач. Для более объективного определения эффективности используется группа общесистемных показателей количества и качества информации:

- полнота добываемой информации;
- своевременность добываемой информации;
- достоверность информации;
- суммарные затраты на получение информации.

Полноту полученной информации можно определить через отношение числа положительных ответов на тематические вопросы к их общему количеству. Тематический вопрос определяет границы информации, необходимой для ответа на этот вопрос. Тематические вопросы можно детализировать до ответов на них в виде «да – нет». Чем выше степень детализации тематических вопросов, тем точнее оценка полноты полученной

информации.

Своевременность информации является важным показателем ее качества, т.к. она влияет на цену информации. Если добытая информация устарела, то затраты на ее добывание оказались напрасными и она не может быть эффективно использована. Поэтому своевременность следует оценивать относительно продолжительности ее жизненного цикла. Если время устаревания информации существенно больше времени ее использования после добывания, то она своевременная, в противном случае она устаревшая.

Нельзя также забывать о том, что *ценность полученной информации определяется результатом ее использования, при этом затраты на получение подобной информации должны быть значительно меньше достигнутого эффекта при ее применении.*

ГЛАВА 9. КАДРОВАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

9.1. Определение кадровой безопасности предприятия
9.2. Особенности отбора персонала
9.3. Обеспечение безопасности предприятия при увольнении персонала

9.1. Определение кадровой безопасности предприятия

Кадровая безопасность – это процесс предотвращения негативных воздействий на экономическую безопасность предприятия за счет рисков и угроз, связанных с персоналом, его интеллектуальным потенциалом и трудовыми отношениями в целом.

Кадровая безопасность занимает доминирующее положение по отношению к другим элементам системы безопасности компании, так как она “работает” с персоналом, кадрами, а они в любой составляющей первичны.

Вся деятельность служб персонала может быть разложена на этапы (поиск, отбор, прием, адаптация и т.д. вплоть до увольнения и далее), и на каждом этапе присутствует масса вопросов безопасности, решаемых именно “кадровиками”. Любое действие менеджера по персоналу на любом этапе – это либо усиление, либо ослабление безопасности компании по главной ее составляющей – по кадрам.

Хотелось бы отметить, что около 80% ущерба материальным активам компаний наносится их собственным персоналом. Только 20% попыток взлома сетей и получения несанкционированного доступа к компьютерной информации приходит извне. Остальные 80% случаев спровоцированы с участием персонала компаний.

Следует различать внешние и внутренние угрозы. Внешние негативные воздействия – это действия, явления или процессы, не зависящие от воли и сознания сотрудников предприятия и влекущие нанесение ущерба. В свою очередь, к внутренним негативным воздействиям относятся действия

(умышленные или неосторожные) сотрудников предприятия, также влекущие нанесение ущерба.

Обеспечение кадровой безопасности является важнейшей составляющей работы менеджера (директора) по персоналу.

Внутренние опасности:

- несоответствие квалификации сотрудников предъявляемым к ним требованиям;
- недостаточная квалификация сотрудников;
- слабая организация системы управления персоналом;
- слабая организация системы обучения;
- неэффективная система мотивации;
- ошибки в планировании ресурсов персонала;
- снижение количества рационализаторских предложений и инициатив;
- уход квалифицированных сотрудников;
- сотрудники ориентированы на решение внутренних тактических задач;
- сотрудники ориентированы на соблюдение интересов подразделения;
- отсутствие или “слабая” корпоративная политика;
- некачественные проверки кандидатов при приеме на работу.

Внешние опасности, связанные с персоналом:

- условия мотивации у конкурентов лучше;
- установка конкурентов на переманивание;
- давление на сотрудников извне;
- попадание сотрудников в различные виды зависимости;
- инфляционные процессы (необходимо учитывать при расчете заработной платы и прогнозировании ее динамики).

Бесспорно, все эти негативные воздействия внешней среды оказывают влияние на процессы внутри предприятия, в целом, на ее безопасность по кадровой составляющей.

Кадровая безопасность зависит от трех основных факторов.

1. *Найм*. Под этим кратким словом понимается целый комплекс мер безопасности при приеме на работу и прогнозирования благонадежности.

2. *Лояльность*. Здесь необходима так называемая «золотая середина». Руководитель, с одной стороны, должен быть снисходителен и доброжелателен к персоналу, для налаживания оптимального психологического климата в организации, с другой стороны, не утрачивать бдительность, чтобы настораживающие моменты не обошли его внимание.

3. *Контроль*. Он представляет собой комплекс мер из установленных для персонала, в том числе для администрации, регламентов, ограничений, режимов, технологических процессов, оценочных, контрольных и других операций, процедур безопасности. Этот комплекс уже непосредственно нацелен на ликвидацию возможностей причинения ущерба и отрабатывается, как правило, службой безопасности или другими подразделениями, но в меньшей степени службой персонала.

С точки зрения безопасности, в подходе к трудовому взаимодействию

необходимо, чтобы каждый кандидат на вакансию, каждый работник предприятия рассматривался, в том числе, и как источник риска, источник потенциальной угрозы. И не только в отношении опасности причинения убытков, связанных с низкой квалификацией, наоборот — с невозможностью применить высокий профессионализм; с недовольством своей работой и условиями труда; с отсутствием четко и однозначно закрепленных юридических правоотношений; с неадекватной оценкой результатов труда; со слабым прогнозированием и контролем благонадежности и т.д.

9.2. Особенности отбора персонала

В настоящее время сложилась практика подбора кадров в коммерческие структуры путем рекомендаций руководителей, сотрудников, знакомых. Нередко на фирмы берутся близкие родственники и друзья. А потом (в 95% случаев) терпят крах родственные и дружеские отношения. Мало кто догадывается, что гораздо выгоднее и безопаснее взять специалиста “со стороны”, но хорошенько его изучить и проверить. А вот как это сделать – с этим мы и постараемся разобраться.

Американский исследователь – президент агентства “Служба коммерческой безопасности” Пол Гоффин разработал концепцию степени риска и квалифицировал людей по группам пониженного, допустимого и высокого риска. Эта концепция сводится к следующему:

- ПОНИЖЕННЫЙ РИСК: люди, которые вряд ли пойдут на компрометацию своей чести и достоинства – 10% от населения США. Наши психологи определили 10% населения России как лиц, которые не воруют.
- ДОПУСТИМЫЙ РИСК: люди, которые могли бы в силу определенных обстоятельств впасть в искушение. Но по своим убеждениям они близки к первой группе. Они не пойдут на преступление, если будут обеспечены соответствующие меры контроля. США – 75%. Наши психологи считают, что в России численность таких кандидатов – 80%.
- ВЫСОКИЙ РИСК: опасные преступники, которые будут создавать условия для хищений, если даже таковые будут отсутствовать. В США таких насчитывается – 15%. Наши психологи относят к этой группе – 10% населения страны.

Изложенные ниже этапы проверки кандидата на работу позволяют отнести его к определенной категории и принять решение о приеме.

Определить идеальные требования для своего кандидата может, наверное, любой руководитель.

Однозначно не пригодны к работе на фирме:

- наркоманы, алкоголики, азартные игроки;
- профессионально некомпетентные работники;
- психически больные, с неустойчивой психикой;
- имеющие связи с криминальными структурами;
- совершавшие особо тяжкие уголовные преступления;

• совершавшие кражи и финансовые банкротства и т.д.

Критерии пригодности могут быть следующими:

• ОБРАЗОВАНИЕ – должно соответствовать установленным требованиям. Знания должны соответствовать диплому.

• ЗДОРОВЬЕ – должны быть отражены любые физические, психологические или умственные недостатки, существенно влияющие на выполнение прямых функциональных обязанностей.

• УПОТРЕБЛЕНИЕ НАРКОТИКОВ ИЛИ СПИРТНОГО – случайное употребление, по праздникам в небольших дозах или систематическое злоупотребление тем и другим.

• ПРИСТРАСТИЕ К АЗАРТНЫМ ИГРАМ – регулярное участие в азартных играх с крупными ставками приводит к недостатку средств и их хищению для удовлетворения своего пристрастия.

• УСТОЙЧИВЫЕ ПРИВЫЧКИ – склонность менять работу, не рассчитываясь с долгами, частые увольнения из-за некомпетентности.

• УГОЛОВНОЕ ПРОШЛОЕ – все обвинения в уголовных правонарушениях и судебно наказуемых поступках в течение последних пяти лет.

• КРАЖИ НА РАБОЧИХ МЕСТАХ – кражи в недалеком прошлом, подделка финансовых документов, получение денег по поддельным документам, очевидные наклонности к хищениям.

• ФИНАНСОВЫЕ АСПЕКТЫ – серьезные финансовые проступки, долги, приписки, финансовые, судебные разбирательства, присвоение денег.

• НЕРАСКРЫТЫЕ ПРАВОНАРУШЕНИЯ – совершенные, но нераскрытые преступления, приобретение краденых товаров, сокрытие доходов, предъявление требований о необоснованных страховых компенсациях, злонамеренная порча материальных ценностей, бегство с места дорожного происшествия, сокрытие найденных денег, хотя их владелец известен, анонимные звонки и т.п.

Для соответствия всем вышеперечисленным требованиям необходимо осуществлять тщательный отбор персонала при приеме на работу.

Отбор кандидатов может осуществляться в несколько этапов.

Этап 1. Изучение анкетных данных кандидата. Необходимо разработать свою анкету или заказать создание анкеты под свои требования специалистам, так как стандартные не всегда и не всем требованиям отвечают.

При этом необходимо помнить, что кандидат может неточно заполнить анкету или вообще опустить компрометирующие его сведения (судимость, увольнение с фирмы за нечестность и т.п.).

Анкета изучается с точки зрения полноты, возможных перерывов в работе, противоречий, проверки по прежним местам работы, месту жительства.

Рекомендуется дополнить анкету следующими вопросами:

1. Материальное благосостояние семьи. Число работающих членов семьи. Объем зарплаты. Совокупный месячный доход семьи (это пригодится при последующей проверке кандидата).

2. Наличие двойного гражданства кандидата и членов его семьи.

3. Реальные причины ухода с прежних мест работы (по крайней мере, с двух-трех последних мест). Впоследствии можно связаться с руководителями фирм, где работал кандидат, и получить на него характеристику, а также узнать причину увольнения.

4. Отношение к спиртному, наркотикам, азартным играм.

5. Увлечения (хобби).

6. Кто из друзей или знакомых может дать ему рекомендацию (ф.и.о., номер телефона).

7. Обращался ли кандидат ранее в какую-либо организацию с просьбой о приеме на работу.

8. Работает ли кандидат где-либо в настоящее время.

9. Имеет ли кандидат возможность ездить в командировки, если это потребуется.

10. Имеет ли кандидат какие-либо физические, умственные или другие медицинские ограничения по предстоящей работе (раскрыть их).

11. Какими видами профессиональной, коммерческой, деловой или общественной деятельности кандидат занимался.

12. Имеется ли у кандидата своя коммерческая или иная фирма.

13. Место прописки и реального проживания.

14. Сведения о жене, муже, родителях, братьях, сестрах.

15. Характерные привычки.

16. Есть ли родственники, друзья за границей.

17. Наличие долгов, неоплаченных счетов, выплата алиментов.

18. Отношение к материальным ценностям, деньгам.

19. Подробные сведения об арестах, судимостях, отбывании наказания, преступных и настораживающих связях, прошлых проблемах криминального характера.

Завершается анкета заявлением о том, что все сообщенные о себе сведения верны и что кандидат предупрежден о недопустимости предоставления о себе ложных сведений.

Этап 2. Если анкетные данные не вызвали каких-либо сомнений, с кандидатом проводится следующая работа.

Собеседование. При собеседовании желательно выявить как положительные, так и отрицательные качества кандидата: конфликтность, повышенная чувствительность, нервозность и т.д. Изучаются коммуникабельность, темперамент, ведущие черты характера, что позволяет прогнозировать поведение человека в разных ситуациях. Выявляется цель поступления на фирму, профессиональный опыт, связи, деловая хватка и другие, необходимые кандидату качества. По результатам собеседование желательно составлять для себя резюме.

Проверка на полиграфе. Для проверки сообщенных кандидатом сведений следует применить к нему специальное психофизиологическое обследование на полиграфе (“детекторе лжи”). Оно позволяет выявить скрываемые факты

биографии, препятствующие зачислению на фирму. Если кандидат успешно прошел данное обследование, то он допускается к следующей стадии проверки.

Тестирование с помощью психологических методик. Выявляются основные психологические черты личности кандидата. Если использовать методики подсознательного уровня, то мы получим довольно объективную картину и сможем спрогнозировать мотивы деятельности в тех или иных ситуациях.

Эта ступень характеризуется, как правило, комплексными психологическими тестированиями. В последнее время значительную популярность приобретают многочисленные методы и процедуры тестирования, поскольку характеризуются быстротой реализации и высокой эффективностью. Каждый из этих методов имеет, конечно, свои ограничения, нарушения которых способны серьезно исказить полученные результаты. Следует при этом особо отметить, что многие тесты, рекомендуемые даже известными научными центрами, составлены все же весьма кустарно и не выдерживают критики. Кроме того, далеко не все методики могут быть рекомендованы к использованию лицами, не имеющими специальной подготовки. Обычно тестовые методики подразделяются на четыре большие группы.

Личностные опросные листы (вопросники). Тесты данного класса представляют собой перечни вопросов, которые требуют от испытуемых лиц однозначно выразить согласие или несогласие с их содержанием. После тестирования ответы анализируются по специальному алгоритму оператором-психоаналитиком. На основе полученных данных формируются психологические характеристики испытуемых претендентов.

Вопросники могут содержать от нескольких десятков до нескольких сотен вопросов. Поэтому по результатам тестирований появляется возможность либо оценить несколько отдельных и наиболее значимых для данной коммерческой структуры психологических качеств конкретной личности, либо составить ее довольно подробный психологический портрет.

К числу типичных вопросов, которые обычно применяются при опросах, относятся, например, следующие:

- готовы ли Вы оказывать помощь другим сотрудникам фирмы (банка) в случае появления у них срочной работы?
- угнетает ли Вас рутинная, кропотливая, повседневная деятельность с документами или иными носителями информации?
- способны ли Вы работать в выходные или праздничные дни в случае возникновения кризисной ситуации в Вашей организации?
- захотите ли Вы прервать свои некоторые социальные контакты и связи, если этого потребует администрация Вашей организации?

При реализации данного метода подкупает кажущаяся порой простота и легкость проведения самого тестирования, а также доступность и быстрота обработки и интерпретации полученных результатов. Но эти якобы короткие сроки и безыскусность процедур весьма обманчивы. При небрежном

отношении к тестированию проводящий его сотрудник, сам того не желая, может допустить грубые методические ошибки и тем самым серьезно исказить конечные результаты. Среди используемых в практике в настоящее время личностных вопросников целесообразно назвать следующие основные тесты.

Тест СМИЛ носит клиническую направленность и предназначен для выявления у испытуемых лиц некоторых психических расстройств и соматических заболеваний. Тест содержит более 500 вопросов. Это вынуждает кандидатов работать с ним достаточно длительное время. Наибольший эффект тест дает в тех случаях, когда требуется диагностировать пограничные состояния психики. Следует обратить особое внимание на то, что из-за низкой, например, квалификации или торопливости проводящих тест операторов существует значительная опасность неправильной интерпретации конечных результатов. В этой связи не рекомендуется использование этого теста для массовых обследований.

Тест КЕТТЕЛА подходит в большей степени для профессионального отбора, так как ориентирован на выявление наличия и степени выраженности, основных 15 психологических особенностей и свойств характера, присущих изучаемому лицу. Тест направлен на выяснение таких качеств личности, как уровень интеллекта, склонность к быстрой смене настроения и пр. По результатам тестирования удается, как правило, составить довольно подробный психологический портрет личности.

Тест АЗЕНКА содержит 57 вопросов и позволяет выявлять такие личностные характеристики, как степень экстравертированности и интравертированности, уровень эмоциональной нестабильности. В сочетании перечисленные характеристики позволяют сделать вывод о темпераменте испытуемого лица.

Тест РСК представляет собой менее известный вопросник, позволяющий определить то, в какой степени испытуемое лицо склонно к принятию рискованных решений в экстремальных ситуациях.

Тест КУ-сорт имеет около 50 утверждений, по реакциям на которые испытуемого лица можно судить о степени его зависимости или независимости от изучаемой малой социальной группы, определять уровень его общительности, выявлять наличие у него потребности к самоутверждению в рамках малой или крупной социальной группы (отдел, подразделение, коммерческая структура) или стремление избегать любых обострений и конфликтных ситуаций.

Характерной особенностью данного теста является то, что он позволяет получать информацию об испытуемом кандидате как при его прямом тестировании (тестируемое лицо само отвечает на все вопросы), так и при заочном тестировании (кто-либо из его близких, друзей, коллег, родственников отвечает на поставленные вопросы как бы от имени тестируемого лица).

Тест ТОМАСА помогает выяснять, а в ряде случаев и прогнозировать поведение кандидата в острых конфликтных ситуациях и чрезвычайных положениях.

Тест УСК позволяет устанавливать уровень субъективного контроля испытуемого лица за развитием событий в жизненно важных для него ситуациях.

Бланковые методики. Эти процедуры представляют собой наборы заданий различной степени сложности, которые предъявляются испытуемому лицу на карточках либо бланках. Кандидат должен найти правильный ответ, выбрав его из предлагаемых ему вариантов, или предложить свой индивидуальный вариант решения задачи. Подобные тесты используются преимущественно для оценки так называемого "индекса интеллекта" либо степени сформированности отдельных психофизиологических функций.

К подобным методикам относятся в первую очередь *тесты РАВЕНА, ВЕКСЛЕРА, АМТХАЭРА, методика компасов, таблицы ШУЛЬТА* и пр. Некоторые из них весьма сложны в обработке и интерпретации результатов, вследствие чего имеют весьма ограниченное применение в практике профессионального отбора в коммерческие структуры.

Вышеперечисленные методики используются главным образом лишь тогда, когда в профессиограмме, например, банка содержатся весьма жесткие и совершенно конкретные требования к тем или иным психофизиологическим качествам будущего сотрудника.

Проективные методики. Эти процедуры являют собой еще более усложненный тип тестов. Полученные с их помощью результаты могут быть достоверно интерпретированы лишь за редким исключением только специалистами, имеющими большой опыт работы с этими методиками. К этой группе тестов относятся *цветовой тест ЛЮШЕРА, пятна РОРХАНА, тест РОЗЕНЦВЕЙГА.*

Приборные методики. Это комплексные процедуры с использованием сложных технических устройств, которые предназначены для всесторонней оценки психофизиологических характеристик испытуемых лиц. В российской практике профессионального отбора кандидатов на работу в коммерческие структуры подобные методики используются пока еще редко, т.к. для их реализации требуются специальные помещения и наличие в составе кадрового подразделения или службы безопасности группы специалистов – психофизиологов.

Следует, однако, отметить, что в последнее время отмечается тенденция к привлечению сторонних экспертов для реализации приборных методик. В подобных случаях это требует, конечно, принятия особых мер безопасности и сохранения конфиденциальности, поскольку сторонние специалисты фактически получают доступ к закрытой внутренней информации коммерческих структур, касающейся кадровых проблем.

Некоторые исследования кандидатов на работу проводят и отдельные российские коммерческие структуры с использованием как отечественной, так и импортной техники. В ряде случаев применяются довольно сложные математические программы для обработки полученных результатов, что, естественно, значительно повышает стоимость таких работ.

В некоторых компьютерных системах ответам испытуемого лица присваивается соответствующих балл, конечно, неизвестный кандидату. В других тестах ответы подвергаются аналитической обработке и в итоге готовятся текстовые заключения о личных и деловых качествах претендента.

В любом случае (оценочно-балльная система, аналитическая версия) вероятностная характеристика и направленность изучаемой личности ложатся в основу подготовки кадровыми подразделениями либо службами безопасности коммерческих структур конкретно-индивидуальных вопросов, которые предстоит поставить перед кандидатом уже в ходе повторного очного интервью.

Методики проверки готовности персонала к действиям в чрезвычайных ситуациях.

Фактически уже сегодня можно констатировать наличие обязательного многоуровневого психологического тестирования с целью выявления подлинных способностей кандидатов действовать четко и без паники в неординарных, экстремальных условиях. Для этого применяются весьма сложные технические системы и комплексы, с помощью которых выявляются характер и масштабы стрессового психофизического состояния личности.

Таким образом, с одной стороны, тестирования дают возможность получать ответы на вопросы, связанные с психологической характеристикой кандидата, что является важным обстоятельством при выработке окончательного решения о его приеме на работу. С другой стороны, в применении тестов необходимо проявлять достаточную осмотрительность и осторожность, поскольку существует вероятность искажения результатов.

Т.о., совокупность этих мер может дать общую характеристику кандидата и сделать первичный вывод о пригодности его для работы в вашей фирме. Результаты изучения кандидата на этих двух этапах позволяют принять решение о прохождении им испытательного срока на фирме.

Этап 3. В течение 3-месячного испытательного срока проверка кандидата должна продолжаться. Проверка может осуществляться через государственные структуры:

- по учетам ГУВД проверяется наличие судимостей, статьи, по которым был осужден кандидат, наличие связей в преступном мире; наличие приводов, исполнение приговоров по административной линии (алименты, штрафы и т.п.);
- по учетам наркологического и психоневрологического диспансеров.

Кроме указанных учетов можно получить сведения на кандидата из следующих источников:

- отделы кадров или руководство фирмы по месту прежней работы;
- общественные организации, в которых состоял кандидат;
- домоуправления, где он проживает;
- школы, вузы, техникумы, где учился кандидат;
- беседы с лицами, которые рекомендовали его на работу.

Этап 4. Во время испытательного срока, а также в период работы

зачисленного в постоянный штат персонала целесообразно проводить различные проверки персонала. Естественно, что в первую очередь должны проверяться те лица, которые по каким-либо причинам вызывают подозрение или недоверие, ведут себя неадекватно обычному сотруднику фирмы, имеют связи среди подозрительных лиц, конкурентов, криминальных элементов.

Рассмотрим различные виды проверок, которые помогут вам обеспечивать кадровую безопасность. Они предполагают возможность контролировать поведение лица при проведении мероприятий, создающих условия, вынуждающие проверяемое лицо действовать в специально для него созданной и легендированной обстановке. Создаваемые условия заставляют проверяемого действовать, предпринимать или не предпринимать те или иные шаги и действия, которые будут свидетельствовать о его честности, лояльности, конспиративности. Или, наоборот, раскроют его негативные стороны.

Проверка на лояльность.

В контракте на работу должна быть записана графа об обязанности сотрудника информировать руководителя фирмы или начальника службы безопасности о попытках вступления с ним в контакт, расспросах о делах фирмы со стороны малознакомых или посторонних лиц. Выявление готовности кандидата в течение испытательного срока написать подобного рода докладную записку является хорошей проверкой будущих сотрудников на лояльность фирме и профилактикой утечки информации.

Лояльность подтверждается также готовностью сотрудника сообщить руководству фирмы ставшие известными сведения о выгодных возможностях и сделках, о попытке конкурентов перехватить контракт, ссуду, кредит.

Лояльность проверяется при сообщениях руководству о подозрительных моментах или признаках готовящихся против фирмы акциях со стороны криминальных структур.

Лояльность проявляется в бережном отношении к имуществу и транспортным средствам фирмы, в стремлении создать, сохранить или укрепить здоровый морально-психологический климат.

Проверка на честность в работе.

В США практикуется следующий метод проверки. Проверяемому создаются все условия, чтобы он мог украсть что-то и был уверен, что кража пройдет незамеченной:

- получение комиссионных с партнера и сокрытие этого факта от руководства фирмы. С партнером же руководства фирмы должна быть договоренность о взаимной проверке своих кадров;
- завышение различных наличных расходов, выданных в подотчет проверяемому сотруднику;
- расходование представительских сумм;
- расходование финансовых средств фирмы на личные нужды без согласования с руководством с последующим их возвратом (когда деньги обесценились);
- использование денег фирмы для спекуляции с валютой;

• закупка валюты и ее продажа после значительного подорожания через определенное время (деньги фирме возвращаются, но уже девальвированные).

Проверка профессиональной пригодности и компетентности.

Проверка проводится обязательно специалистом в этой же отрасли знаний или деятельности. Проверка может проводиться:

• путем собеседования по проблеме;

• путем поручения выполнить ту или иную работу.

Проверка на возможные связи с криминальными структурами.

• предложения помощи руководству фирмы в возврате кредитов и долгов нетрадиционными методами;

• жаргон, близкий к криминальному;

• излишняя самоуверенность в вопросах личной безопасности;

• тюремные наколки;

• скрытный сбор компрометирующих материалов на руководящих сотрудников фирмы;

• работа по совместительству, требующая соответствующих знаний или информации.

Проверка на соблюдение коммерческой тайны.

• проверка случаев срывов контрактов;

• выявление в беседах с партнерами их осведомленности о делах и планах фирмы после встреч с их представителями сотрудника фирмы;

• утрата сотрудником документов фирмы, содержащих коммерческую тайну;

• работа с секретными документами фирмы дома или в вечернее (нерабочее) время без согласования с руководством;

• перехват конкурентами сделок, контракта, о которых было известно на фирме ограниченному кругу лиц.

Проверка на наличие компрометирующих материалов.

• сбор данных о прошлой жизни и деятельности проверяемого из бесед с его начальником, товарищами по работе, компаньонами, конкурентами;

• личные неосторожные высказывания в беседах о каких-либо событиях и делах, компрометирующих проверяемого, последующая их проверка, возможное документирование;

• подделка платежного поручения, подделка подписей при получении зарплаты за кого-либо из сотрудников;

• стремление избегать в разговорах тем, касающихся прошлой деятельности сотрудника, его жизни;

• излишняя скрытность, настороженность в поведении;

• наличие наколок, использование “лагерного языка” и сокрытие факта судимости.

Проверка на наличие пагубных увлечений.

• наблюдение за сотрудником на праздничных приемах, презентациях, встречах с партнерами и т.п. Рано или поздно пристрастие к спиртному проявится;

- наблюдение за состоянием сотрудника после праздничных дней, выходных и т.п.;
- неестественное поведение, блеск в глазах у наркоманов. Подавленность, сменяющаяся беспричинным радужным настроением;
- внезапное исчезновение или появление денег у игрока;
- разговоры об играх, скачках, картах, рулетке и т.д.

Проверка на работу на свою или другую фирму с использованием служебных возможностей.

Здесь, наряду с проведением комбинаций по проверке, можно проконтролировать доходы и расходы сотрудника.

В предварительных ознакомительных беседах с кандидатом целесообразно осторожно выяснить его финансовое и материальное положение: наличие счетов в банках, совокупный месячный доход семьи.

Затем, в ходе работы, следует уточнить эти данные, перепроверить правильность первоначально полученных сведений. Естественно, что все это должно делаться деликатно, чтобы не вызвать подозрений и не оскорбить своего сотрудника. Иногда такие беседы можно проводить в ходе праздничного стола, когда внимание и бдительность под влиянием спиртного и общего доброжелательного настроения значительно ослабевают. Кроме того, необходимо сравнить доходы и расходы сотрудника в течение года. Если его расходы значительно выше официальных доходов – это серьезный сигнал для глубокой проверки.

Прежде всего необходимо выяснить источники дополнительных доходов. Это может быть работа по совместительству без согласования с руководством фирмы. Особенно когда знания и информация, получаемая на фирме, позволяют лучше или полностью исполнять обязанности по совместительству.

Проверка на болтливость.

При собеседовании с кандидатом выясните его предыдущее место работы и расспросите подробно о той фирме, где работал кандидат. В перечень вопросов включите и вопросы, содержащие коммерческую тайну той фирмы. Если кандидат “откровенно” все расскажет, нужно выяснить причину такого поведения, возможно, он будет так же разговорчив и о новом месте работы.

Необходимо подчеркнуть, что психологический отбор рекомендуется осуществлять всегда в сочетании с другими приемами изучения кандидатов.

В последние годы в ведущих московских коммерческих банках широко практикуется *почерковедческая экспертиза*, которая позволяет определить многие черты характера кандидата: темперамент, выдержку, волевые качества, собранность, аккуратность, грамотность, общеобразовательный уровень и пр., а также предрасположенность к совершению неблаговидных и нечестных поступков.

По мнению экспертов, даже каждый, взятый в отдельности из упомянутых методов проверки достаточно эффективен. В совокупности же достигается весьма высокая степень достоверности информации о профессиональной пригодности и надежности кандидата, способности к творческой работе на

конкретном участке в соответствующей коммерческой структуре.

9.3. Обеспечение безопасности предприятия при увольнении персонала

Серьезное влияние на вопросы безопасности коммерческих структур оказывают процедуры увольнения сотрудников. К сожалению, отдельных руководителей порой мало интересуют чувства и переживания персонала, который по тем или иным причинам попадает под сокращение. Как показывает опыт, такой подход приводит, как правило, к серьезным негативным последствиям.

Современные психологические подходы к процессу увольнения позволяют выработать следующую принципиальную рекомендацию: *какие бы ни были причины увольнения сотрудника, он должен покидать коммерческую организацию без чувства обиды, раздражения и мести.* Только в этом случае можно надеяться на то, что увольняемый сотрудник не предпримет необдуманных шагов и не проинформирует правоохранительные органы, налоговую инспекцию, конкурентов, криминальные структуры об известных ему подлинных или мнимых недостатках, промахах, ошибках в деятельности его прежних руководителей.

Таким образом, представители кадровых служб должны быть четко ориентированы на выяснение истинных мотивов увольнения всех категорий сотрудников. Зачастую причины, на которые ссылается сотрудник при увольнении, и подлинные мотивы, побудившие его к такому шагу, существенно отличаются друг от друга. Обычно ложный защитный мотив используется потому, что сотрудник в силу прежних привычек и традиций опасается неправильной интерпретации своих действий со стороны руководителей и коллег по работе. Наряду с этим весьма часто имеют место случаи, когда сотрудник внутренне сам уверен в том, что увольняется по откровенно называемой им причине, хотя его решение сформировано и принято под влиянием совершенно иных, порой скрытых от него обстоятельств.

В этой связи принципиальная задача состоит в том, чтобы определить истинную причину увольнения сотрудника, попытаться правильно ее оценить и решить, целесообразно ли в данной ситуации предпринимать попытки к искусственному удержанию данного лица в коллективе, либо отработать и реализовать процедуру его спокойного и бесконфликтного увольнения. Решение рекомендуется принимать на основе строго объективных данных в отношении каждого конкретного сотрудника.

При поступлении устного или письменного заявления об увольнении рекомендуется во всех без исключения случаях провести беседу с участием представителя кадрового подразделения и кого-либо из руководителей коммерческой структуры. До беседы целесообразно предпринять меры по сбору следующей информации об увольняющемся сотруднике:

- характер его взаимоотношений с коллегами в коллективе;

- отношение к работе;
- уровень профессиональной подготовки;
- наличие конфликтов личного или служебного характера;
- ранее имевшие место высказывания или пожелания перейти на другое место работы;
- доступ к информации, в т.ч. составляющей коммерческую тайну;
- вероятный период устаревания сведений, составляющих коммерческую тайну;
- предполагаемое в будущем место работы увольняющегося (увольняемого) сотрудника.

Беседа при увольнении проводится лишь только после того, когда собраны все необходимые сведения. Конечно, предварительно руководитель коммерческой структуры отрабатывает принципиальный подход к вопросу о том, целесообразно ли предпринимать попытки склонить сотрудника изменить его первоначальное решение либо санкционировать оформление его увольнения. В любом случае рекомендуется дать собеседнику высказаться и в развернутой форме объяснить мотивы своего решения. При выборе места проведения беседы предпочтение отдается, как правило, служебным помещениям.

В зависимости от предполагаемого результата, беседа может проводиться в официальном тоне либо иметь форму доверительной беседы, задушевного разговора, обмена мнениями. Однако, каковы бы ни были планы в отношении данного сотрудника, разговор с ним должен быть построен таким образом, чтобы последний ни в коей мере не испытывал чувства униженности, обиды, оскорбленного достоинства. Для этого следует сохранять тон беседы предельно корректным, тактичным и доброжелательным, даже несмотря на любые критические и несправедливые замечания, которые могут быть высказаны сотрудником в адрес коммерческой структуры и ее конкретных руководителей.

Если правлением банка (фирмы), отделом кадров и службой безопасности все же принято решение не препятствовать увольнению сотрудника, а по своему служебному положению он располагал доступом к конфиденциальной информации, то в этом случае отрабатывается несколько вариантов сохранения в тайне коммерческих сведений (оформление официальной подписки о неразглашении данных, составляющих коммерческую тайну, либо устная "джентльменская" договоренность о сохранении увольняемым сотрудником лояльности к "своему банку или фирме").

В этой связи необходимо подчеркнуть, что личностное обращение к чувству чести и достоинства увольняемых лиц наиболее эффективно в отношении тех индивидуумов, которые обладают темпераментом сангвиника и флегматика, высоко оценивающих, как правило, доверие и доброжелательность.

Что касается лиц с темпераментом холерика, то с этой категорией сотрудников рекомендуется завершать беседу на официальной ноте. В ряде случаев объявление им принятого решения об увольнении вызывает бурную

негативную реакцию, связанную с попытками спекулировать на своих истинных, а порой и мнимых профессиональных достоинствах. Поэтому с сотрудниками такого темперамента и склада характера целесообразно тщательно оговаривать и обусловливать в документах возможности наступления для них юридических последствий раскрытия коммерческой тайны.

Несколько иначе рекомендуется действовать в тех случаях, когда увольнения сотрудников происходят по инициативе коммерческих структур. В этих обстоятельствах не следует поспешно реализовывать принятое решение. Если увольняемое лицо располагает какими-либо сведениями, представляющими коммерческую тайну, то целесообразно предварительно и под соответствующим предлогом перевести его на другой участок работы, т.е. в такое подразделение, в котором отсутствует подобная информация.

Кроме того, таких лиц традиционно стремятся сохранить в структуре банка или фирмы до тех пор, пока не будут приняты меры к снижению возможного ущерба от разглашения ими сведений, составляющих коммерческую тайну, либо найдены адекватные средства защиты конфиденциальных данных (технические, административные, патентные, юридические, финансовые и пр.).

Только лишь после реализации этих мер рекомендуется приглашать на собеседование подлежащего увольнению сотрудника и объявлять конкретные причины, по которым коммерческая структура отказывается от его услуг. Желательно при этом, чтобы эти причины содержали элементы объективности, достоверности и проверяемости (перепрофилирование производства, сокращение персонала, ухудшение финансового положения, отсутствие заказчиков и пр.). *При мотивации увольнения целесообразно, как правило, воздерживаться от ссылок на негативные деловые и личные качества данного сотрудника.*

После объявления об увольнении рекомендуется внимательно выслушивать контрдоводы, аргументы и замечания сотрудника в отношении характера работы, стиля руководства компанией и т.п. Обычно увольняемый персонал весьма критично, остро и правдиво освещает ситуацию в коммерческих структурах, вскрывая уязвимые места, серьезные недоработки, кадровые просчеты, финансовые неурядицы и т.п.

Если подходить непредвзято и объективно к подобной критике, то эти соображения могут быть использованы в дальнейшем весьма эффективно в интересах фирмы или банка. В ряде случаев увольняемому сотруднику предлагают даже изложить письменно свои рекомендации, конечно, за соответствующее вознаграждение.

Кроме того, такая беседа позволяет выработать решение о целесообразности предоставления увольняемому лицу каких-либо рекомендательных документов для трудоустройства на новом месте работы. Следует категорически избегать каких-либо намеков о сведении личных счетов с увольняемым кандидатом за его прежние недостатки в работе и поведении.

При окончательном расчете обычно рекомендуется независимо от

личностных характеристик увольняемых сотрудников отбирать у них подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работ.

В любом случае после увольнения сотрудников, осведомленных о сведениях, составляющих коммерческую тайну, целесообразно через возможности службы безопасности банка или фирмы (частного детективного агентства) проводить оперативную установку по их новому месту работы и моделировать возможности утечки конфиденциальных данных.

Кроме этого, в наиболее острых и конфликтных ситуациях увольнения персонала проводятся оперативные и профилактические мероприятия по месту работы, жительства также в окружении носителей коммерческих секретов.

ВОПРОСЫ К ЗАЧЕТУ по дисциплине «Безопасность предпринимательской деятельности»

1. Предпринимательская деятельность как объект посягательств
2. Основные понятия безопасности
3. Комплексная безопасность предприятия
4. Формы взаимоотношений субъектов рынка
5. Виды экономических угроз
6. Социальные и политические угрозы
7. Информационные угрозы
8. Коррупция как фактор угроз предпринимательству
9. Правовые угрозы
10. Криминальные угрозы
11. Хозяйственные преступления
12. Правовая защита
13. Организационная защита
14. Инженерно-техническая защита
15. Универсальные меры обеспечения безопасности предприятия
16. Цели, задачи, функции службы безопасности
17. Структура службы безопасности
18. Основные задачи режима и охраны
19. Требования внутриобъектового режима
20. Организация пропускного режима
21. Виды пропусков
22. Общие положения перевозки грузов различными транспортными средствами
23. Организация охраны грузов на железнодорожном транспорте
24. Организация охраны грузов, перевозимых автомобильным транспортом
25. Охрана грузов при использовании воздушного транспорта
26. Основные направления компьютерных преступлений
27. Классификация компьютерных преступлений
28. Защита компьютерных данных

29. Роль разведки в обеспечении экономической безопасности предприятия
30. Информационные потребности предприятия
31. Разведка конкурентов
32. Планирование разведывательной деятельности
33. Виды и методы разведки
34. Принципы и технология добывания информации
35. Определение эффективности добывания информации
36. Определение кадровой безопасности предприятия
37. Особенности отбора персонала
38. Обеспечение безопасности предприятия при увольнении персонала

ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ КОНТРОЛЬНЫХ РАБОТ по дисциплине «Безопасность предпринимательской деятельности»

В соответствии с учебным планом студенты заочной и ускоренной формы обучения направления «Менеджмент», изучающие дисциплину «Безопасность предпринимательской деятельности», должны выполнить контрольную работу.

Контрольная работа является важной составной частью учебно-исследовательской работы студента и предназначена для углубленного изучения проблематики дисциплины, закрепления пройденного материала, развития индивидуальных творческих способностей студента.

Контрольная работа выполняется в форме реферата и оформляется в соответствии с нижеобозначенными требованиями.

Задачами работы студента над рефератом являются:

- углубленное изучение выбранной темы;
- приобретение умения вести поиск необходимого фактического материала, его анализа и систематизации, формулирования научных выводов;
- приобретение навыков грамотного и логически доказательного изложения текста, правильности оформления работы и приложений.

Реферат представляет собой исследование по отдельной теме (вопросу) дисциплины и пишется, как правило, на основе опубликованных источников и научной литературы. Отражает одну некрупную проблему, умение вести анализ, сравнивать мнения авторов, делать выводы, иметь свою точку зрения.

Одновременно реферат может содержать анализ имеющихся в распоряжении студента нормативных, лекционных и других материалов, их творческое обобщение и систематизацию.

Каждая тема посвящена сложным специфическим проблемам безопасности предпринимательской деятельности.

При подготовке контрольных работ следует привлечь учебную и монографическую литературу, законодательные и инструктивные материалы по предложенным темам, выпущенным Правительством и Парламентом РФ, статистические и информационные материалы, публикуемые в экономической и другой прессе РФ, а также справочную литературу, публикации в таких

специальных журналах, как «Защита и безопасность», «Защита информации», «Алгоритм безопасности», «Охранная деятельность», «Мир безопасности», «Охранные системы», «Частный сыск. Охрана. Безопасность», «Бизнес и безопасность в России», «Вопросы защиты информации», «Системы безопасности» и некоторые другие. Возможно также использовать при написании работы материалы Интернет – источников.

Контрольная работа выполняется на белых листах формата А4 без рамок (210х297 мм). Допускается применение отдельных листов формата А3 (297х420 мм) для иллюстраций, таблиц, распечаток. Контрольная работа помещается в скоросшиватель. Объем работы: 15-20 машинописных листов формата А4 с одной стороны. Текст набирается в редакторе MS Word. Шрифт Times New Roman. Размер шрифта основного текста – 14. Отступы красной строки – 10 мм. Пустые строки (абзацы) не допускаются. Межстрочный интервал полуторный, выравнивание текста – по ширине страницы. Текст контрольного задания следует набирать, соблюдая следующие размеры полей: левое – 30 мм, правое – 10 мм, верхнее и нижнее – по 20 мм. Наиболее важные слова, фразы, предложения и абзацы в тексте допускается выделять курсивом. Необходимо также соблюдать равномерную плотность, контрастность и четкость текста по всей работе. В работе должны быть четкие, не расплывшиеся линии, буквы, цифры и знаки. Все линии, буквы, цифры и знаки должны быть одинаково черными по всей работе.

На титульном листе содержится информация о министерской подчиненности образовательного учреждения, о полном наименовании учебного заведения, наименование кафедры преподавателя; наименование изучаемой дисциплины; тематика работы; фамилия, инициалы и группа студента; фамилия, инициалы, ученая степень и звание преподавателя; город и год сдачи работы.

Страницы контрольной работы следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту. Номер страницы проставляется в середине нижнего поля страницы без точки в конце. Титульный лист включается в общую нумерацию страниц, но номер страницы на нем не ставится. Иллюстрации, таблицы, расположенные на отдельных листах, включаются в общую нумерацию страниц.

Для создания формул, рисунков и таблиц используются встроенные возможности MS Word. Нумеруются последовательно в пределах главы и включают номер главы и порядковый номер рисунка в главе (например, рис. 2.3). Каждый рисунок должен иметь название рядом с номером. Рисунок должен следовать сразу после ссылки на него в тексте. Аналогичным образом оформляются таблицы.

В списке литературы на первом месте указываются Конституция и законы РФ, законы Алтайского края, затем – подзаконные акты (указы Президента РФ, постановления Правительства РФ, нормативные акты министерств и ведомств), акты органов местного самоуправления, статистические справочники, сборники документов и материалов, другие документальные публикации. После законов

и подзаконных актов в алфавитном порядке перечисляют учебники, учебные пособия, монографии, статьи и тезисы в сборниках, журналах, газетах, словарях и энциклопедиях, авторефераты диссертаций, депонированные рукописи, статистические, инструктивные и отчетные материалы предприятий, организаций, учреждений, ссылки на интернет – источники и т.д.. Каждый источник должен быть соответствующим образом описан. Описание каждого источника должно включать фамилию и инициалы автора (авторов), полное наименование книги или статьи без кавычек; название, год, номер журнала и страницы, на которых расположена статья (для статей); вид книги (учебник, учебное пособие, монография, автореферат диссертации и т.п.), город издания, издательство, год издания, общее количество страниц. Все источники в списке литературы должны быть новыми (не старше пяти лет). Список использованной литературы должен содержать не менее 10 источников. Библиографическое описание книги удобнее всего выполнять непосредственно по библиографическому описанию этой книги, располагающемуся, как правило, на ее второй странице над аннотацией. За образец можно взять оформление списка учебно-методических материалов по дисциплине к данному пособию.

На все указанные в списке литературы источники должны быть ссылки в работе. Ссылка также должна производиться на каждую цитату, цифру или факт на этой же странице внутри текста. Ссылки оформляются следующим образом: в квадратных скобках необходимо указывать номер цитируемого источника по списку литературы и номер страницы: например, [2, с. 56]. Точка в конце предложения ставится после ссылки.

Реферат должен содержать:

1. Введение – где студенты должны отразить актуальность выбранной тематики, цели и задачи реферата.

2. Основная часть. Не менее 2-3 разделов в соответствии с выбранной или заданной темой реферата.

3. Заключение – где студенты должны подвести итог проделанного исследования.

Защиту реферата принимает преподаватель дисциплины. Если реферат не допущен к защите, он возвращается студенту вместе с рецензией на доработку.

Контрольная работа должна быть сдана преподавателю на проверку не позднее, чем за неделю до начала сессии, после чего происходит ее защита в форме индивидуального собеседования.

Выбор номера варианта индивидуального задания осуществляется в соответствии с номером зачетной книжки студента.

ВАРИАНТЫ КОНТРОЛЬНЫХ ЗАДАНИЙ по дисциплине «Безопасность предпринимательской деятельности»

1. Виды экономических преступлений.
2. Государственное регулирование в области защиты информации.

3. Виды угроз информационным объектам и безопасности информации.
4. Организация инженерно-технической защиты информации на предприятии.
5. Понятие, проблемы и структура экономической безопасности предпринимательской деятельности (на примере фирм различных типов).
6. Информационная безопасность, история формирования.
7. Правовые основы институтов тайны.
8. Коммерческая тайна в системе экономической безопасности.
9. Коммерческая тайна и конкуренция.
10. Разработка перечня сведений, составляющих коммерческую тайну.
11. Организация защиты информации, составляющей коммерческую тайну предприятия.
12. Разработка программы защиты информации, составляющей коммерческую тайну.
13. Обеспечение безопасности информации, составляющей коммерческую тайну.
14. Особенности работы с персоналом, владеющим информацией, относимой к коммерческой тайне.
15. Пути достижения безопасности коммерческого предприятия и основные направления обеспечения безопасности коммерческого предприятия.
16. Правовые и законодательные основы обеспечения безопасности коммерческого предприятия.
17. Коммерческая тайна как одна из основных форм обеспечения безопасности предприятия.
18. План мероприятий по защите коммерческих секретов предприятия.
19. Инженерно-техническая защита, понятие и средства.
20. Универсальные меры обеспечения безопасности предприятия.
21. Основные виды угроз интересам предприятия.
22. Цель деятельности службы безопасности. Основные задачи службы безопасности.
23. Функции службы безопасности. Структура службы безопасности.
24. Понятие режима и охраны (основные задачи организации режима и охраны, цели, задачи и принципы режима и охраны).
25. Организация пропускного режима (понятие контрольно-пропускного режима, основные цели пропускного режима, пропускные документы).
26. Основы разработки системы защиты объекта (оценка эффективности системы защиты объекта, факторы, влияющие на выбор приемов и средств охраны, виды охраны, виды стационарных объектов, рубежи охраны, охрана территории объекта, охрана помещений).
27. Причины роста уязвимости предпринимателей от экономических преступлений.
28. Основные направления по обеспечению экономической безопасности предприятия.
29. Формы проявления недобросовестной конкуренции.

30. Группы информации, составляющие коммерческую тайну предприятия, и их состав.

31. Понятие системы защиты информации. Основные требования к организации эффективного функционирования системы защиты информации.

32. Люди как источники конфиденциальной информации.

33. Человеческий фактор как основа системы защиты информации.

34. Основные направления отбора кадров в современных условиях, с целью обеспечения безопасности предприятия.

35. Группы организационных мероприятий по работе с персоналом, получающим доступ к конфиденциальной информации.

36. Концепция информационной безопасности.

37. Основы экономической безопасности предпринимательской деятельности.

38. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

39. Правовые основы защиты конфиденциальной информации.

40. Экономические основы защиты конфиденциальной информации.

41. Организационные основы защиты конфиденциальной информации.

42. Хранение конфиденциальных документов.

43. Направления и методы защиты аудио- и визуальных документов.

44. Виды и назначение технических средств защиты информации, в помещениях, используемых для проведения переговоров.

45. Анализ опыта защиты информации в зарубежных странах.

46. Основы технологии обработки и хранения конфиденциальных документов

47. Назначение, виды, структура и технология функционирования системы защиты информации.

48. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

49. Направления и методы защиты профессиональной тайны.

50. Направления и методы защиты служебной тайны.

51. Защита секретов в дореволюционной России.

52. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.

53. Порядок подбора персонала для работы с конфиденциальными документами.

54. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.

55. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.

56. Классификация посетителей фирмы, характеристика каждой группы.

57. Защита информации в рекламной и выставочной деятельности.

58. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

59. Назначение, виды и технология учета конфиденциальных документов.
60. Анализ существующих схем доступа персонала в помещения фирмы.
61. Аналитический обзор российского и зарубежного опыта в предотвращении утраты ценной информации по вине сотрудников.
62. Психологические и профессиональные особенности личности человека, владеющего тайной, мотивация мышления и поведения.
63. Факторы, предпосылки и условия применения различных форм материального и морального стимулирования ответственного отношения сотрудников к обеспечению информационной безопасности фирмы.
64. Место и роль психологического климата в коллективе при проведении воспитательной работы в коллективе фирмы.
65. Классификация противоправных действий персонала фирмы.
66. Преступления в сфере компьютерной информации.
67. Характеристика систем обеспечения информационной безопасности.
68. Компьютерная преступность и компьютерная безопасность.
69. Криптографические системы защиты информации.
70. Технические средства несанкционированного доступа к информации.
71. Аналитическая работа в сфере безопасности информационных ресурсов.
72. Проблемы обеспечения безопасности в компьютерных сетях.
73. Защита информации в работе кадровой службы.
74. Современные технические средства охраны помещений, офисов и других объектов от проникновения посторонних лиц.
75. Обеспечение безопасности внешнеэкономической деятельности предприятия (фирмы).
76. Проблемы информационной безопасности.
77. Виды защиты информации в компьютерных сетях.
78. Информационное оружие.
79. Секреты фирмы и методы их похищения.
80. Юридические и экономические аспекты обеспечения безопасности предпринимательской деятельности.
81. Контроль над экономической преступностью в России.
82. Нелегальный рынок и характеристика основных нелегальных рынков.
83. Понятие, структура и масштабы теневой экономики.
84. Методы выявления и оценки параметров теневой и криминальной экономики.
85. Законодательство РФ, регулирующее предпринимательскую деятельность.
86. Основные транснациональные преступные организации и транснациональная организованная преступность в России.
87. Преступления против правил конкуренции в России.
88. Криминогенные условия и преступность в сфере внешнеэкономической деятельности в России.
89. Отмывание денег в России.

90. Предпринимательская деятельность как объект неправомерных посягательств.
91. Рейдерство в России и зарубежом.
92. Демпинг и борьба с ним.
93. Промышленный шпионаж и способы защиты от него.
94. Недобросовестная конкуренция.
95. Оффшорные территории и экономическая преступность.
96. Защита интеллектуальной собственности.
97. Интернет – преступления в предпринимательской деятельности.
98. Посягательства на интересы сотовых компаний.

УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Нормативно-правовые акты

1. Конституция Российской Федерации (с изменениями, внесенными Указами Президента от 9 января 1996 года № 0 и от 10 февраля 1996 года №173) // РГ от 25.12.93; 13.01.96; 15.02.96.
2. Закон РФ от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» (в ред. Федеральных законов от 02.02.2006 № 19-ФЗ, от 18.12.2006 №231-ФЗ, от 24.07.2007 № 214-ФЗ) // РГ от 5.08.2004.

Основная литература

1. Русецкая, Э.А. Страхование в системе экономической безопасности России / Э.А. Русецкая. - М. ; Берлин : Директ-Медиа, 2014. 168 с http://biblioclub.ru/index.php?page=book&id=271713&sr=1
2. Суглобов, А.Е. Экономическая безопасность предприятия: учебное пособие / А.Е. Суглобов, С.А. Хмелев, Е.А. Орлова. - М.: Юнити-Дана, 2013.-272 с. http://biblioclub.ru/index.php?page=book&id=118957&sr=1
3. Экономическая безопасность : учебное пособие / В.А. Богомолов, Н.Д. Эриашвили, Е.Н. Барикаев и др. ; под ред. В.А. Богомолов. - 2-е изд., перераб. и доп. - М. : Юнити-Дана, 2012. - 296 с.
http://biblioclub.ru/index.php?page=book&id=11828**2&sr=1**

Дополнительная литература

1. Богомолов В.А. Экономическая безопасность: [текст]: учеб. пособие/ В.А. Богомолов. - М.: ЮНИТИ, 2006. - 303 с. Экземпляры: всего:5 - ХР(4), ЧЗ(1)
2. Вечканов Г.С. Экономическая безопасность: [текст] Учебник/ Г.С. Вечканов. - М.: Питер, 2007. - 374 с. Экземпляры: всего:5 - ЧЗ(1), ХР(4)
3. Кузнецов И.Н. Бизнес-безопасность: [текст] Учебник/ И.Н. Кузнецов. – 3-е изд. – М.: Издательско-торговая корпорация «Дашков и К», 2010.-416 с. Экземпляры: всего:19 - ЧЗ(1), ХР(18)
4. Коробкина Е.В. Безопасность предпринимательской деятельности: Курс лекций: Учебно-методическое пособие по подготовке к зачету и выполнению контрольной работы для студентов заочной формы обучения специальности 080507 «Менеджмент организации» / Рубцовский индустриальный институт. – Рубцовск, 2010. - 111 с. Экземпляров-30.
5. Бизнес-разведка. Внедрение передовых технологий [Текст]: пер. с англ. / Кристофер Боган, Майкл Инглиш; под общей редакцией Б.Л. Резниченко. – М.: Вершина, 2006. – 368 с.
6. Ярочкин В.И. Система безопасности фирмы [Текст]: Учебник / В.И. Ярочкин. – 3-е изд., перераб. и доп. – М.: Ось-89, 2005. – 352 с.
7. Доронин А.И. Бизнес-разведка [Текст]: Учебник / А.И. Доронин. – 4-е изд., М.: Ось-89, 2007. – 528 с. (Серия «Секьюрити»)

Программное обеспечение и Интернет-ресурсы

1. Сервер органов государственной власти РФ http://www.gov.ru/

2. Верховный суд Российской Федерации http://www.supcourt.ru
3. Конституционный суд РФ http://ks.rfnet.ru/
4. Высший арбитражный суд РФ http://www.arbitr.ru
5. Министерство внутренних дел РФ http://www.mvdinform.ru/
6. Министерство информационных технологий и связи РФ http://www.minsvyaz.ru/
7. Министерство РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий http://www.mchs.gov.ru/
8. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам http://www.fips.ru/rospatent/index.htm
9. Предпринимательское право http://businesspravo.ru/
10. Система Гарант http://www.garant.ru/
11. Консультант Плюс http://www.consultant.ru/
12. http://www.ist.ru/vp/cgi-bin/request.exe
13. Российский сервер по безопасности http://www.secur.ru
14. Весь Рынок Безопасности России - Sec.Ru http://www.sec.ru/
15. Технические средства безопасности http://uks.dol.ru/
16. «Территория взлома» http://www.hackzone.ru/
17. ОХРАНА.RU http://www.oxpaha.ru/
18. Журнал «Защита информации. Конфидент» http://www.confident.ru/magazine
19. «БДИ» (Безопасность, Достоверность, Информация) : http://www.bdi.spb.ru/
20. «Бизнес и Безопасность» http://www.bsm.com.ua/
21. Журнал «Охранные системы» http://www.magazine.security.com.ua
22. «Центр информационной безопасности Маском» http://www.mascom.ru/
23. Союз Независимых Служб содействия коммерческой безопасности http://www.usc.ru/

Периодические издания:

- ✓ «Проблемы теории и практики управления»,
- ✓ «Менеджмент в России и за рубежом»,
- ✓ «Ползуновский вестник»,
- ✓ «Управление персоналом»,
- ✓ «Российский экономический журнал»,
- ✓ «ЭКО»,
- ✓ «Защита и безопасность»,
- ✓ «Защита информации»,
- ✓ «Алгоритм безопасности»,
- ✓ «Охранная деятельность»,
- ✓ «Мир безопасности»,
- ✓ «Охранные системы»,
- ✓ «Частный сыск. Охрана. Безопасность»,
- ✓ «Бизнес и безопасность в России»,
- ✓ «Вопросы защиты информации»,
- ✓ «Системы безопасности» и др.

СЛОВАРЬ

Антикоррупционные меры контроля над организованной преступностью – обучение государственных чиновников правилам общественно значимого поведения (нормам публичной этики), ужесточение правил заключения государственных контрактов, сокращение бюрократического аппарата, утверждение принципа свободы печати, формирование общественного мнения, скандальные разоблачения, запрет на выдвижение лиц с криминальным прошлым в качестве кандидатов на выборные должности, совершенствование способов аудита.

Банковская тайна – информация, доступ к которой банк, в соответствии с законом, имеет право ограничивать.

Безопасность предпринимательской деятельности – 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.

Виды организованной преступной деятельности – рэкет, преступное ростовщичество, отмывание денег, кража интеллектуальной собственности, морское пиратство, угон самолетов, захват наземного транспорта, мошенничество, компьютерная преступность, экологическая преступность, торговля людьми, торговля человеческими органами, незаконная торговля наркотиками, ложное банкротство, проникновение в легальный бизнес, коррупция и подкуп общественных и партийных деятелей, выборных лиц.

Внутренний аудит – деятельность по проверке и контролю, анализу и оценке финансового состояния фирмы, осуществляемая собственными работниками фирмы (предприятия) в целях предупреждения негативных тенденций в финансово-хозяйственной деятельности фирмы, выявления имеющихся нарушений и своевременного принятия мер по их ликвидации.

Внутренний сопоставительный анализ деятельности предприятия – метод экономического анализа, основанный на сопоставлении сравнимых показателей деятельности предприятия за ряд периодов времени. Данный метод эффективен для выявления скрытых доходов, отмывания денег. Корректное применение метода предполагает относительное постоянство условий экономической деятельности предприятия в течение длительного периода времени.

Гарантии предпринимательской деятельности – система законодательно закрепленных положений, направленных на обеспечение

нормального функционирование, развития и защиты предпринимательства от противоправных посягательств.

Генерирование криминального дохода – фаза криминального экономического цикла, содержанием которой является извлечение дохода в результате преступной (общественно опасной) экономической деятельности, совершение преступлений в сфере экономики.

Диффузная (стихийная) транснациональная преступность – экономические транснациональные преступления, совершаемые отдельными лицами или группами лиц и носящие случайный эпизодический характер: контрабандный вывоз из страны частным лицом валюты, драгоценных металлов либо каких-либо ценностей, сокрытия имущества при разводе через оффшорные компании и т.п.

Доминирующее положение на рынке – исключительное положение хозяйствующего субъекта или нескольких хозяйствующих субъектов на рынке товара, не имеющего заменителя, либо взаимозаменяемых товаров, дающее ему возможность оказывать решающее влияние на общие условия обращения товара на соответствующем товарном рынке или затруднять доступ на рынок другим хозяйствующим субъектам.

Заведомо ложная реклама – использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей (исполнителей, продавцов).

Клонирование – преступная схема посягательства на интересы компаний сотовой телефонной связи, основанная на том, что абонент использует чужой идентификационный номер (а следовательно, – и счет) в корыстных интересах. При этом используется следующая последовательность действий:

1. Преступник перехватывает идентифицирующий сигнал чужого телефона и выделяет из него идентификационные номера MIN и ESN. Потенциальный преступник может перехватить эту электронную информацию при помощи радиосканера либо так называемого сотового кэш-бокса, представляющего собой комбинацию сканнера, компьютера и сотового телефона. Он легко выявляет и запоминает номера MIN и ESN и автоматически перепрограммирует себя на них. Использовав пару MIN/ESN один раз, он стирает ее из памяти и выбирает другую. Такой аппарат делает выявление мошенничества практически невозможным. Несмотря на то, что эта аппаратура на Западе пока еще редка и дорога, она уже существует и представляет растущую опасность для пользователей сотовой связи.

2. Преступник перепрограммирует свой телефон так, чтобы пользоваться электронным серийным номером и телефонным номером этого абонента. Перепрограммирование осуществляется путем перенесения информации с помощью компьютера на микросхему, которая вставляется в сотовый телефон. Таким телефоном можно пользоваться до тех пор, пока несанкционированные вызовы не будут обнаружены. Стоимость разговора с этого аппарата заносится базовой станцией на счет того абонента, у которого эти номера были украдены.

3. Доказав, что такие вызовы были произведены не им, абонент может опротестовать счета и добиться их отмены. В таких случаях компания сотовой связи вынуждена оплатить междугородную часть таких вызовов. Преступник же выходит на номер любого другого абонента и снова возвращается к своему незаконному бизнесу.

Коммерческая тайна – 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.

Коммерческий шпионаж – действия лиц, направленные на незаконное получение коммерческой информации, находящейся под защитой.

Комплексная система обеспечения экономической безопасности предпринимательства – это совокупность мероприятий организационно-правового характера, осуществляемых в целях защиты предпринимательской деятельности от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным экономическим потерям.

Коммерческий подкуп – незаконная передача лицу, выполняющему управленческие функции в коммерческой или иной организации, денег, ценных бумаг, иного имущества, а равно незаконное оказание ему услуг имущественного характера за совершение действий (бездействия) в интересах дающего в связи с занимаемым этим лицом служебным положением.

Компьютерная преступность охватывает преступления, совершаемые с помощью компьютеров, информационно вычислительных систем и средств телекоммуникаций или направленные против них с корыстными либо некоторыми другими целями.

Конфиденциальная информация – документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Контрабанда – перемещение в крупном размере через таможенную границу Российской Федерации товаров или иных предметов, за исключением указанных в части второй 188 статьи УК РФ, совершенное помимо или с сокрытием от таможенного контроля либо с обманным использованием документов или средств таможенной идентификации либо сопряженное с недекларированием или недостоверным декларированием.

Контроль над экономической преступностью – регламентированная нормами права деятельность государственных, муниципальных органов, а

также негосударственных организаций, направленная на предупреждение, выявление и пресечение нарушения правовых норм, обеспечивающих нормальное функционирование экономической системы.

Криминальная экономика – 1) непродуктивный сектор экономической деятельности, связанный с незаконным перераспределением доходов и имущества граждан путем грабежа, разбоя, кражи, вымогательства; 2) специфический экономический уклад, способ хозяйствования, который призван обеспечивать определенную, относительно небольшую по численности группу лиц сверхдоходами, доходами от преступной деятельности, доходами от использования "прорех" в законодательстве"; 3) экономические отношения, экономическая деятельность, главным отличительным признаком которой является общественная вредность (опасность); 4) система социально-экономических институтов, то есть формальных и неформальных правил экономического поведения, а также санкционных механизмов.

Криминальный экономический цикл – процесс последовательной смены отдельных стадий криминальной экономической деятельности, необходимых для ее осуществления и постоянного возобновления. Эти стадии инвариантны конкретному содержанию любой систематически и планомерно реализуемой преступной деятельности в сфере экономики. Основными стадиями подобной модели являются: генерирование преступного дохода, легализация или отмывание криминальных фондов, потребление, криминальное инвестирование преступных доходов и инфильтрация их в легальный бизнес.

Криминальные инвестиции – фаза криминального экономического цикла, связанная с использованием легализованных преступно полученных средств для возобновления, расширения криминального предприятия.

Легализация (отмывание) денежных средств или иного имущества, приобретенных незаконным путем – совершение финансовых операций и других сделок с денежными средствами или иным имуществом, приобретенными заведомо незаконным путем, а равно использование указанных средств или иного имущества для осуществления предпринимательской или иной экономической деятельности.

Лжепредпринимательство – создание коммерческой организации без намерения осуществлять предпринимательскую или банковскую деятельность, имеющее целью получение кредитов, освобождение от налогов, извлечение иной имущественной выгоды или прикрытие запрещенной деятельности.

Международные преступления – преступления против мира и безопасности человечества, представляющие повышенную опасность для всего человечества. К ним относятся агрессия, геноцид, апартеид, насильственное

установление или сохранение колониального господства, применение ядерного оружия, расизм, терроризм и т.п.

Меры предупреждения и пресечения легализации доходов от криминальной экономической деятельности:

- определение понятия легализации (отмывания) доходов как деятельности по приданию правомерного вида доходам, полученным преступным путем;
- признание преступлением любых действий по легализации (отмыванию) финансовых средств, полученных преступным путем, с установлением соответствующей ответственности и конфискацией таких средств;
- установление требований по регистрации некоторых видов финансовых операций и идентификации лиц, их совершающих, а также требований к хранению этих материалов;
- использование широкого понятия финансовой операции, охватывающего операции с деньгами, ценными бумагами, имуществом, имущественными правами, а также удостоверение и регистрацию таких операций;
- применение широкого понятия организации, осуществляющей финансовые операции, в качестве которой должны признаваться не только кредитные организации, но и все другие хозяйствующие субъекты, а равно учреждения связи, игорные заведения и др.;
- ограничение коммерческой и банковской тайны в целях получения информации, необходимой для выявления и пресечения действий по легализации (отмыванию) доходов от преступной деятельности;
- установление ограничений на финансовые операции с наличными деньгами и перемещение наличных денег через таможенную границу;
- введение категории финансовых операций, подлежащих особому контролю (подозрительных операций);
- установление обязанности работников организаций, осуществляющих финансовые операции, сообщать уполномоченному органу о незаконных операциях и операциях, требующих особого контроля;
- иммунитет работников организаций, осуществляющих финансовые операции, от ответственности за разглашение сведений, составляющих коммерческую или банковскую тайну, при сообщении таких сведений уполномоченному органу в предусмотренных законом случаях;
- установление ответственности работников организаций, осуществляющих финансовые операции:
  - за отказ от предоставления уполномоченным органам сведений о незаконных операциях или операциях, требующих особого контроля;
  - за разглашение информации о предоставлении таких сведений;
  - за невыполнение требования о регистрации финансовых операций и лиц, их совершающих, а также за уничтожение таких документов;
  - за нарушение правил работы с наличными деньгами и др.

Методы интеграции преступно полученных доходов: продажа

недвижимости, искажение цен внешнеторговых сделок; сделки с занижением цены, сделки с завышением цены; трансферпрайсинг; использование банковских счетов иностранной или совместной фирмы; депонирование наличности на банковский счет фирмы; подставные компании и ложные кредиты; “отмывшие” через казино и лотереи; установление контроля над иностранными банками.

Методы размещения преступно полученных доходов с использованием традиционных финансовых организаций: смерфинг – превращение наличных денег в финансовые инструменты; обмен мелких банкнот на купюры более крупного достоинства; обменные сделки – организованный обмен денег на купюры иного достоинства или другую валюту; структурирование операций с наличными деньгами; установление контроля над финансовыми учреждениями; незаконное использование исключений из закона; использование корреспондентских отношений между банками; создание ложного бумажного следа; слияние законных и незаконных фондов; перевод преступно полученных денег за рубеж; использование “коллективных” счетов; использование транзитных счетов; механизм гарантии ссуды (ссылки на части этого же файла).

Монопольно высокая цена – цена товара, устанавливаемая хозяйствующим субъектом, занимающим доминирующее положение на товарном рынке, с целью компенсации необоснованных затрат, вызванных недоиспользованием производственных мощностей и (или) получения дополнительной прибыли в результате снижения качества товара.

Монопольно низкая цена – цена приобретаемого товара, устанавливаемая хозяйствующим субъектом, занимающим доминирующее положение на товарном рынке в качестве покупателя, в целях получения дополнительной прибыли и (или) компенсации необоснованных затрат за счет продавца, или цена товара, сознательно устанавливаемая хозяйствующим субъектом, занимающим доминирующее положение на товарном рынке в качестве продавца, на уровне, приносящем убытки от продажи данного товара, с целью ограничения конкуренции посредством вытеснения конкурентов с рынка.

Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Мошенничество с использованием банков (Prime Bank Fraud) – заключаются в том, что мошенники, прикрываясь именами и гарантиями известных и респектабельных финансовых учреждений, предлагают инвесторам вложение денег в ничем не обеспеченные обязательства с нереальными размерами доходности.

Мошенничество с абонементом – преступная схема посягательства на

интересы компаний сотовой телефонной связи, включающая следующие стадии:

1. Преступник абонирует сотовую связь на имя другого лица без ведома последнего;
2. Преступник предлагает своим клиентам анонимно звонить в любую точку мира по низкому тарифу;
3. Если счет остается неоплаченным, телефон отключается. Мошенник подключается к очередному чужому номеру;
4. Компании сотовой связи вынуждены возмещать компаниям междугородной связи стоимость таких звонков.

Навязывание информации (Touting) – введение инвесторов в заблуждение недостоверной информацией об эмитенте, преувеличенными перспективами роста компаний, ценные бумаги которых предлагаются. Анонимность, которую предоставляет своим пользователям сеть Интернет, возможность охвата большой аудитории, высокая скорость и гораздо более низкая стоимость распространения информации по сравнению с традиционными средствами делает Интернет наиболее удобным инструментом для мошеннических действий.

Налоговая преступность – общественно опасное социально-правовое явление, включающее в себя совокупность преступлений, объектом которых являются охраняемые уголовным законом отношения по поводу взимания налогов и иных обязательных платежей, а также осуществления контроля за своевременностью и полнотой их уплаты.

Недобросовестная конкуренция – 1) злоупотребление правом свободной конкуренции для извлечения прибыли; 2) любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и могут причинить или причинили убытки другим хозяйствующим субъектам – конкурентам либо нанести ущерб их деловой репутации.

Незаконная банковская деятельность – осуществление банковской деятельности (банковских операций) без регистрации или без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением условий лицензирования.

Незаконное предпринимательство – осуществление предпринимательской деятельности без регистрации либо без специального разрешения (лицензии) в случаях, когда такое разрешение (лицензия) обязательно, или с нарушением условий лицензирования.

Незаконное получение кредита – получение индивидуальным предпринимателем или руководителем организации кредита либо льготных условий кредитования путем представления банку или иному кредитору заведомо ложных сведений о хозяйственном положении либо финансовом состоянии индивидуального предпринимателя или организации.

Нелегальный рынок – совокупность отношений, осуществляющихся в нарушение действующих правовых норм и сводящих вместе покупателей и продавцов товаров и услуг. Нелегальный рынок является базовым институтом теневой и криминальной экономики.

Нелегальный экспорт капитала – 1) осуществляемое в нарушение правовых норм помещение капитала за границу в денежной или товарной форме, через сферу услуг (в том числе в форме патентов, лицензий, ноу-хау), ведущее к образованию иностранной собственности за рубежом или иной формы обязательств, дающих право на получение прибыли; 2) незаконное перечисление средств резидентом нерезиденту с переходом прав собственности на них; 3) совершение капитальных валютных операций по перевозке, вывозу и пересылке валютных ценностей в нарушение лицензионного порядка, установленного Центральным банком России.

Неправомерные действия при банкротстве (статья 195 УК РФ) – действия, связанные с совершением следующих деяний: 1) сокрытие имущества или имущественных обязательств; 2) сокрытие сведений об имуществе, о его размере, местонахождении либо иной информации об имуществе; 3) передача имущества в иное владение; 4) отчуждение имущества; 5) уничтожение имущества; 6) сокрытие, уничтожение, фальсификация бухгалтерских и иных учетных документов, отражающих экономическую деятельность, если эти действия совершены руководителем или собственником организации – должника либо индивидуальным предпринимателем при банкротстве или в предвидении банкротства и причинили крупный ущерб; 7) неправомерное удовлетворение имущественных требований отдельных кредиторов руководителем или собственником организации – должника либо индивидуальным предпринимателем, знающим о своей фактической несостоятельности (банкротстве), заведомо в ущерб другим кредиторам, а равно принятие такого удовлетворения кредитором, знающим об отданном ему предпочтении несостоятельным должником в ущерб другим кредиторам, если эти действия причинили крупный ущерб.

Нецелевое использование средств государственных финансовых фондов – такое их использование, которое не приводит к результатам, предусмотренным при их выделении, или приводит к этим результатам, но сопровождается неправомерными действиями или событиями. Такая неправомерность может быть закреплена в правовых актах, в заключаемых

договорах, в решениях полномочных органов, определяющих целевой характер выделяемых из федерального бюджета средств.

Обман потребителей – обмеривание, обвешивание, обсчет, введение в заблуждение относительно потребительских свойств или качества товара (услуги) или иной обман потребителей в организациях, осуществляющих реализацию товаров или оказывающих услуги населению, а равно гражданами, зарегистрированными в качестве индивидуальных предпринимателей в сфере торговли (услуг).

Ограничение конкуренции – принятие нарушающих права участников рынка актов и иных действий федеральных органов государственной власти, органов исполнительной власти субъектов РФ и органов местного самоуправления, а также соглашений хозяйствующих субъектов между собой. Осуществляется в следующих формах: ограничение конкуренции путем раздела рынка; соглашения и согласованные действия, направленные на раздел рынка; ограничение доступа на рынок; устранение с рынка других субъектов экономической деятельности; установление единых цен; поддержание единых цен.

Организованная преступность корыстного типа (mercenery crime) – организованная преступная деятельность, осуществляемая с целью получения непосредственной материальной выгоды. Связана с совершением таких преступлений, как грабежи, кражи, рэкет, мошенничество и другие.

Отмывание денег – 1) процесс, посредством которого скрывается существование, незаконное происхождение или незаконное использование доходов, и затем эти доходы маскируются таким образом, чтобы казаться имеющими законное происхождение; 2) это процесс, в ходе которого средства, полученные в результате незаконной деятельности, то есть различных правонарушений, помещаются, переводятся или иным образом пропускаются через финансово-кредитную систему (банки, иные финансовые институты), либо на них (вместо них) приобретается иное имущество, либо они иным образом используются в экономической деятельности и в результате возвращаются владельцу в ином “воспроизведенном” виде для создания видимости законности полученных доходов, сокрытия лица, инициировавшего данные действия и (или) получившего доходы, а также противозаконности источников этих средств (Страсбургская конвенция и рекомендации Специальной финансовой комиссии по проблемам отмывания денег).

Оффшорная зона – любая страна с низкой или нулевой налоговой ставкой на все или отдельные категории доходов, определенный уровень банковской или коммерческой секретности, и минимальное или полное отсутствие резервных требований Центрального банка или ограничений по

конвертируемости валюты. Большинство оффшорных зон имеют относительно простые требования по лицензированию и регулированию финансовых и иных компаний и фирм.

Оффшорная фирма (компания) – термин, характеризующий особый организационно-юридический статус предприятия, которое обеспечивает ему максимальное снижение налоговых платежей, финансовую секретность и конфиденциальность операций.

Параллельная (вторгающаяся) экономика – теневые отношения, не связанные с официальным экономическим статусом их участников, особый сектор с особой производственной функцией, где занята без официальной регистрации часть рабочей силы.

Перепрограммирование – преступная схема посягательства на интересы компаний сотовой телефонной связи, включающая следующие стадии:

1) Преступник приобретает сотовый телефонный аппарат законным способом и заменяет микросхему или же нелегально приобретает телефон с уже перепрограммированным программным запоминающим устройством (ПЗУ); 2) При помощи перепрограммированного аппарата преступник получает доступ к коммутационному оборудованию телефонных компаний, и его вызовы обрабатываются, как и любые другие, с той лишь разницей, что предъявить по ним счет некому; 3) Поскольку компания сотовой связи не может установить личность клиента, она вынуждена оплатить счета по стоимости междугородной части таких вызовов. Если такая махинация проведена на высоком уровне, данный тип мошенничества невозможно отследить или предотвратить.

Преднамеренное банкротство – умышленное создание или увеличение неплатежеспособности, совершенное руководителем или собственником коммерческой организации, а равно индивидуальным предпринимателем в личных интересах или интересах иных лиц, причинившее крупный ущерб либо иные тяжкие последствия (статья 196 УК РФ).

Предпринимательская деятельность – самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке.

Признаки экономической преступности – 1) корыстный характер; 2) совершение в процессе профессиональной деятельности; 3) связана с договорами и обязательствами; 4) коллективность жертв; 5) анонимность жертв; 6) наличие двух субъектов - юридического (преступность корпораций) и физического лиц (преступность по роду занятости), действующих от имени и в интересах предприятия; 7) существенный ущерб, причиняемый экономическим интересам государства, частного предпринимательства и граждан; 8) множественный характер; 9) перераспределение материальных благ как

следствие экономических преступлений; 10) длящийся, систематический характер.

Присвоение или растрата – хищение чужого имущества, вверенного виновному.

Присвоение авторства – выпуск в полном объеме или части чужого произведения под своим именем, а также издание под своим именем произведения, созданного в соавторстве с другими лицами, без указания их фамилий.

Причины возникновения и развития нелегальных рынков:

- наличие правового запрета на обращение товаров, реализацию услуг, выполнение работ (наркотические средства, трансплантаты, краденое имущество, отмывание преступно полученных доходов);
- наличие установленных законодательством барьеров для доступа на рынок (государственная монополия, лицензирование, возрастные ограничения для малолетних на рынке труда, авторские права, защита интеллектуальной собственности (патент, товарный знак));
- государственное регулирование цен (установление максимальных цен, ограничение рентабельности, установление фиксированного валютного курса на уровне, ниже равновесного);
- высокий уровень налогообложения и других издержек, связанных с исполнением установленных законом обязательств;
- недостаточная жесткость государственного контроля, неспособность государства реализовать правовой запрет либо исполнение регулирующих предписаний.
- недееспособность государственных институтов регулирования рынка, обеспечения прав собственности, контрактной дисциплины (например, неэффективность судебной системы разрешения споров, исполнения судебных решений, связанных с истребованием долгов порождают рынок криминальных услуг по их “выбиванию”).

Размещение (p1acement) – стадия процесса отмывания денег, связанная с физическим размещением наличных денежных средств в мобильные финансовые инструменты, территориальное удаление от мест их происхождения. Размещение осуществляется в традиционных финансовых учреждениях, нетрадиционных финансовых учреждениях, розничной торговле либо полностью за пределами страны.

Расслоение (layering) – стадия процесса отмывания денег, направленная на отрыв незаконных доходов от их источников путем сложной цепи финансовых операций, направленных на маскировку проверяемого следа этих доходов. Различные финансовые операции наслаиваются одна на другую с целью

усложнить работу правоохранительных органов по отысканию незаконных фондов, подлежащих конфискации.

Стратегия экономической безопасности – долгосрочный подход к достижению цели, выражаемый через общую концепцию комплексной системы обеспечения экономической безопасности предпринимательской деятельности.

Субъекты комплексной системы обеспечения экономической безопасности предпринимательства – физические и юридические лица, органы государственной власти, прямо либо опосредованно обеспечивающие защищенность предпринимательской деятельности от внешних и внутренних угроз.

Социально-правовой контроль над экономической преступностью – деятельность по контролю над противоправным поведением в сфере экономики, осуществляемая государственными органами и институтами гражданского общества, преследующая цель эффективного воздействия на криминогенные факторы, детерминанты экономической преступности.

Синдикализированная организованная преступность (преступный синдикат) – вид организованной преступной деятельности, осуществляемой с целью получения максимальной прибыли путем незаконного производства товаров и услуг и совершения экономических преступлений с использованием мафия-метода.

Структура криминальной экономики – совокупность входящих в ее состав элементов, сфер, секторов:

- незаконные экономические отношения в сфере легальной экономической деятельности (экономическая преступность и адмделиктность);
- скрытая экономика – разрешенная законом деятельность, которая официально не показывается или приуменьшается осуществляющими ее субъектами в целях уклонения от уплаты налогов, внесения социальных взносов или от выполнения определенных законом обязательств;
- сфера нелегального бизнеса, связанного с производством, реализацией и потреблением нормальных товаров и услуг без лицензии и специального разрешения;
- сфера нелегальной (неформальной – в терминологии СНС-93) занятости;
- сфера нелегального бизнеса, связанного с производством, реализацией и потреблением запрещенных товаров и услуг, при котором имеет место трудовой процесс, а выпускаемые товары и услуги имеют эффективный рыночный спрос;
- сфера уголовного промысла, в рамках которой криминальные доходы извлекаются на базе систематического совершения традиционных общеуголовных преступлений (профессиональная преступность);

- сфера услуг, связанных с применением или угрозой применения насилия в экономических отношениях (заказные убийства, криминальный терроризм). Цель данного вида деятельности – силовое обеспечение функционирования криминальной экономики, подавление конкуренции и социального контроля насильственными методами, посредством совершения общеуголовных преступлений. Развитие данной сферы связано с коммерциализацией общеуголовной насильственной преступности;
- сфера создания, толкования, применения, исполнения теневых (неформальных) норм, регулирующих сферу криминальной экономической деятельности;
- незаконные экономические отношения в сфере политического рынка, политической деятельности;
- незаконные экономические отношения в системе государственной и муниципальной службы в связи с осуществлением экономической деятельности, принятием и исполнением экономически значимых решений.

Схема "увеличить и сбросить" (Pump&dump) – вид манипуляции на рынке ценных бумаг, заключающейся в извлечении прибыли за счет продажи ценных бумаг, спрос на которые был искусственно сформирован. Манипулятор, называясь инсайдером или осведомленным лицом и распространяя зачастую ложную информацию об эмитенте, создает повышенный спрос на определенные ценные бумаги, способствует повышению их цены, затем осуществляет продажу ценных бумаг по завышенным ценам. После совершения подобных манипуляций цена на рынке возвращается к своему исходному уровню, а рядовые инвесторы оказываются в убытке. Используется в сети Интернет.

Схема финансовой пирамиды (Pyramid Schemes) – классическая финансовая пирамида с использованием Интернет – технологий. При использовании данного приема инвестор получает прибыль исключительно за счет вовлечения в игру новых инвесторов.

Схема "надежного" вложения капитала (The "Risk - free" Fraud) – заключается в распространении через Интернет инвестиционных предложений с низким уровнем риска и высоким уровнем прибыли. Как правило, это предложение несуществующих, но очень популярных проектов, таких как вложения в высоколиквидные ценные бумаги банков, телекоммуникационных компаний, в сочетании с безусловными гарантиями возврата вложенного капитала и высокими прибылями.

Тактика обеспечения безопасности – применение конкретных процедур и выполнение конкретных действий в целях обеспечения экономической безопасности субъекта предпринимательства.

Теневая экономика (учетно-статистическое понятие) – представляет собой сферу экономической деятельности, включающей следующие элементы:

1) Законная деятельность, скрываемая или приуменьшаемая производителями в целях уклонения от уплаты налогов или выполнения других обязательств;

2) Неформальная (неофициальная легальная) деятельность, в том числе:

- деятельность некорпорированных (то есть непосредственно принадлежащих одному владельцу, часто – семейных) предприятий, работающих для собственных нужд, то есть производство товаров и услуг, произведенных в домашних хозяйствах и ими же потребленных;
- деятельность некорпорированных предприятий с неформальной занятостью (временные бригады строителей и т.п.);

3) Неофициальная нелегальная деятельность, в том числе:

- легальные виды деятельности, которыми занимаются нелегально (например, без лицензий и специальных разрешений);
- нелегальная деятельность, представляющая собой запрещенные законом производство и распространение товаров и услуг, на которые имеется эффективный рыночный спрос (производство и распространение наркотиков, проституция, контрабанда).

Теневая экономика – 1) экономика, функционирующая вне правового поля. Ее ключевым признаком можно считать уклонение от официальной регистрации коммерческих договоров или умышленное искажение их при регистрации. Основным методом реализации подобных отношений начинает выступать насилие или его угроза субъектам сделок (О. Исправников); 2) неконтролируемый обществом сектор общественного воспроизводства в ходе производства, распределения, обмена и потребления экономических благ и предпринимательских способностей, скрываемых от органов государственного управления и контроля экономических отношений между хозяйствующими субъектами по использованию государственной, негосударственной и криминально нажитой собственности в целях извлечения сверхдоходов (сверхприбыли) для удовлетворения личных и групповых потребностей небольшой части населения страны (В.М. Есипов); 3) фактически не контролируемое обществом производство, распределение, обмен и потребление товарно-материальных ценностей и услуг (С.Д. Головнин).

Теневые операции – скрываемые сделки (трансакции), а также учетные, расчетные, информационные процедуры, а также прочие действия (различные скрытые соглашения, организационные, коммуникативные, физические действия):

а) хозяйственные операции (технологические, производственные, трудовые, маркетинговые, сбытовые, операции по материально-техническому обеспечению, торговые и ряд других);

б) финансовые операции (расчетные, кредитные, фондовые, валютные, страховые);

в) учетные операции, связанные с осуществлением бухгалтерского, управленческого, статистического учета экономической деятельности.

Транснациональная бизнес-преступность – преступления, направленные на систематическое получение прибыли посредством преступного использования международных экономических отношений. Данный вид преступности является наиболее опасным и совершается организациями самых различных типов (как преступными, так и легальными), а также группами лиц и отдельными лицами. Отличается такими признаками, как функциональность, структурированность и институциональный характер.

Транснациональная преступность – преступность, выходящая за границы одного государства. В структуре транснациональной преступности традиционно выделяют три элемента: международные преступления, преступления международного характера и преступления, связанные с иностранцами.

Транснациональные преступления (виды): отмывание денег; терроризм; кражи произведений искусства и предметов культуры; кража интеллектуальной собственности; незаконная торговля оружием; угон самолетов; морское пиратство; захват наземного транспорта; мошенничество со страховкой; компьютерная преступность; экологическая преступность; торговля людьми; торговля человеческими органами; незаконная торговля наркотиками; ложное банкротство; проникновение в легальный бизнес; коррупция и подкуп общественных и партийных деятелей, выборных лиц.

Угрозы экономической безопасности предпринимательства – потенциальные или реальные действия физических или юридических лиц, нарушающие состояние защищенности субъекта предпринимательской деятельности и способные привести к прекращению его деятельности либо к экономическим и другим потерям.

Фиктивное банкротство – заведомо ложное объявление руководителем или собственником коммерческой организации, а равно индивидуальным предпринимателем о своей несостоятельности в целях введения в заблуждение кредиторов для получения отсрочки или рассрочки причитающихся кредиторам платежей или скидки с долгов, а равно для неуплаты долгов, если это деяние причинило крупный ущерб.

Финансовая преступность – совокупность преступлений, непосредственно связанных с посягательством на отношения по формированию, распределению, перераспределению и использованию фондов

денежных средств (финансовых ресурсов) субъектов экономических отношений.

Финансовый контроль – это регламентированная нормами права деятельность государственных, муниципальных, общественных и иных субъектов по проверке своевременности и точности финансового планирования, обоснованности и полноты поступления доходов в соответствующие фонды денежных средств, правильности и эффективности их использования.

Цель комплексной системы обеспечения экономической безопасности предпринимательства – минимизация внешних и внутренних угроз экономическому состоянию субъекта предпринимательства, в том числе его финансовым, материальным, информационным, кадровым ресурсам, на основе разработанного и реализуемого комплекса мероприятий экономико-правового и организационного характера.

Экономическая преступность – 1) преступления, совершаемые корпорациями против государственной экономики, против других корпораций служащими корпораций против самой корпорации, корпорациями против потребителей (Лунеев В.В.); 2) противоправная деятельность, посягающая на интересы экономики государства в целом, а также на частнопредпринимательскую деятельность и на интересы отдельных групп граждан, постоянно и систематически осуществляемая с целью извлечения наживы в рамках и под прикрытием законной экономической деятельности как физическим, так и юридическим лицом (Дементьева Е.Е.); 3) совокупность корыстных преступлений, совершаемых в сфере экономики лицами в процессе их профессиональной деятельности, в связи с этой деятельностью и посягающих на собственность и другие интересы потребителей, партнеров, конкурентов и государства, а также на порядок управления экономикой в различных отраслях хозяйства (Э.И. Петров, Р.Н. Марченко, Л.В. Баринова); 4) уголовно наказуемые виновные общественно опасные деяния, посягающие или использующие легальные экономические институты, то есть правила, формы, процедуры, контрольные и санкционные механизмы экономической деятельности.

Юрисдикционная форма защиты прав и законных интересов предпринимателя от неправомерных действий – обращение предпринимателя за защитой к государственным или иным уполномоченным органам (суд, арбитражный суд, третейский суд), которые принимают необходимые меры для восстановления нарушенных прав и пресечения правонарушения.

Коробкина Елена Владимировна

БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Курс лекций

Учебное пособие для студентов очной и заочной
форм обучения направления «Менеджмент»

Редактор Е.Ф. Изотова

Подписано к печати 18.12.15. Формат 60х84 /16.
Усл. печ. л. 7,13. Тираж 40 экз. Заказ 151507. Рег. №137.

Отпечатано в ИТО Рубцовского индустриального института
658207, Рубцовск, ул. Тракторная, 2/6.