Федеральное агентство по образованию

Государственное образовательное учреждение
высшего профессионального образования
«ЧЕЛЯБИНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт экономики отраслей, бизнеса и администрирования
Кафедра экономики отраслей и рынков

Бархатов В.И., Бархатов И.В.,
Капкаев Ю.Ш., Супроненко Д.Л.

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Под редакцией В.И. Бархатова

Челябинск
ЧелГУ
2007

Экономическая безопасность: Учебное пособие / В.И. Бархатов, И.В. Бархатов, Ю.Ш. Капкаев, Д.Л. Супроненко и др.; Под ред. д.э.н., профессора В.И. Бархатова– Челябинск

В учебном пособии изложены теоретические основы экономическо-хозяйственной деятельности предприятия как системы обобщенных знаний о содержании, функциях, принципах организации финансов предприятия.

Также в пособии рассматриваются вопросы расходов и доходов предприятий, формирования и планирования финансового результата.

В пособии освещено формирование капитала, его структуры и цены. Особое внимание уделено вопросам оценки и анализа экономического потенциала предприятия, а также анализу результативности финансово-хозяйственной деятельности предприятия.

Учебное пособие предназначено для студентов высших учебных заведений, обучающихся по специальностям 060500 «Бухгалтерский учет, анализ и аудит»,060400 «Финансы и кредит», 060600 «Мировая экономика», специалистов предприятий.

АВТОРСКИЙ КОЛЛЕКТИВ
Бархатов В.И., Бархатов И.В.,
Капкаев Ю.Ш., Супроненко Д.Л.

СОДЕРЖАНИЕ

Глава 1. Служба экономической безопасности предприятия

Ключевые понятия:

Безопасность	Системность
Система безопасности	Концепция безопасности
Угроза безопасности	Физическая безопасность
Объект безопасности	Информационная безопасность
Законность	Экономическая безопасность
Гласность	Экологическая безопасность
Конспирация	Психологическая безопасность
Компетентность	Зоны защиты

1.1 Общие положения

Созданию службы безопасности предприятия обычно предшествуют два события: либо это острое желание руководителей предприятия отреагировать на внезапно возникшие реальные угрозы имуществу, физической расправы с персоналом и т.д., либо это основанный на результатах исследования вывод о неудовлетворительном состоянии безопасности предприятия. В первом случае созданная поспешно служба безопасности способна в некоторой степени отразить угрозы и в дальнейшем реагировать на их появление по принципу «угроза - отражение». Дело меняется существенным образом при реализации второго варианта. После детального изучения состояния безопасности предприятия (с привлечением специалистов, если их нет на предприятии) у его руководителей появится реальное представление о системе безопасности предприятия. Такое системное представление (зафиксированное в письменной форме) позволяет осознанно и целенаправленно проводить работу по обеспечению безопасности предпринимательской деятельности и самого предприятия всеми его подразделениями и сотрудниками. При этом ведущая роль службы безопасности не исчезает, наоборот, понимание своей роли и места в системе безопасности предприятия приведет только к положительным результатам.

Следует, однако, подчеркнуть, что до настоящего времени нет единого подхода к определению понятия «система безопасности предприятия». Чтобы дать такое определение, необходимо предварительно выявить элементы этой системы. Структурными элементами системы безопасности предприятия являются научная теория его безопасности, политика и стратегия безопасности, средства и методы обеспечения безопасности и, наконец, концепция безопасности предприятия.

Совокупность вышеперечисленных элементов составляет **систему безопасности** предприятия.

Под **безопасностью** следует понимать состояние объекта (в нашем случае - предприятия) в системе его связей с точки зрения способности к устойчивости (самовыживанию) и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов.

Под **угрозой** безопасности предприятия следует понимать потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности.

Угрозу можно классифицировать по различным основаниям и измерить их в количественных параметрах. Например, возможный ущерб оценивается числом погибших людей, потерявших (ухудшивших) здоровье, денежной сумме

экономических потерь и т.д. **Классификация угроз** безопасности организации по различным основаниям приведена в таблице 1.1.

Функции безопасности по отношению к угрозам можно разделить на следующие (Рисунок 1.1):

Рисунок 1.1 – Разделение функций безопасности по отношению к угрозам

Под **объектом** безопасности предприятия следует понимать степень устойчивости и развития предприятия, его способность противостоять угрозам. В объекте безопасности предприятия можно выделить:

- различные структурные подразделения или группы сотрудников либо владельцы акций предприятия;
- ресурсы предприятия (информационные, кадровые, материально-технические, информационные, интеллектуальные и финансовые);
- различные виды деятельности (управленческая, производственная, снабженческая и т.д.).

Целью обеспечения безопасности предприятия является комплексное воздействие на потенциальные и реальные угрозы, позволяющее ему успешно функционировать в нестабильных условиях внешней и внутренней среды.

Достижение этой цели требует реализации следующих **задач**:

1. Выявление угроз для стабильности и развития предприятия и выработка мер по их противодействию;
2. Обеспечение защиты технологических процессов;
3. Реализация мер противодействия всех видов шпионажа (промышленного, научно-технического, экономического и т.д.);
4. Своевременное информирование руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;
5. Предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;
6. Всестороннее изучение деловых партнеров;
7. Своевременное выявление и адекватное реагирование на дезинформационные мероприятия;
8. Разработка и совершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия;
9. Реализация мер по защите коммерческой и иной информации;

Таблица 1.1 -Классификация угроз безопасности организации

По степени вероятности	⁎ невероятная ⁎ маловероятная ⁎ вероятная ⁎ весьма вероятная ⁎ вполне вероятная
По степени развития	⁎ возникновение (зарождение) ⁎ экспансия ⁎ стабилизация ⁎ ликвидация
Отдаленность угрозы во времени	⁎ непосредственная ⁎ близкая (до 1 года) ⁎ далекая (свыше 1 года)
Отдаленность угрозы в пространстве	⁎ территория предприятия ⁎ прилегающая к предприятию ⁎ территория ⁎ территория региона ⁎ территория страны ⁎ зарубежная территория
Темпы нарастания угрозы	⁎ месяцы ⁎ кварталы ⁎ годы
Напряженность угрозы	⁎ нормальная ⁎ повышенная ⁎ близкая к пределу (порог) ⁎ избыточная
По природе возникновения	⁎ естественные (объективные), т.е. вызванные стихийными природными явлениями, не зависящими от человека (наводнения, землетрясения, ураганы и т.п.) ⁎ искусственные (субъективные), т.е. вызванные деятельностью человека непреднамеренные (неумышленные) и преднамеренные (умышленные) угрозы
По источнику возникновения	⁎ экономические ⁎ социальные ⁎ правовые ⁎ организационные ⁎ информационные ⁎ экологические ⁎ технические ⁎ криминальные

10. Организация мероприятий по противодействию недобросовестной конкуренции;

11. Обеспечение защиты всех видов ресурсов предприятия;

12. Реализация мер по защите интеллектуальной собственности;

13. Организация и проведение мер по предотвращению чрезвычайных ситуаций;

14. Выявление негативных тенденции среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих

рекомендаций;

15. Выявление негативных тенденции среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих рекомендаций;

16. Организация взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;

17. Разработка и реализация мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;

18. Возмещение материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц.

Система безопасности предприятия может быть построена на основе следующих **принципов**:

1) **Приоритет мер предупреждения**. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

2) **Законность**. Меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

3) **Комплексное использование сил и средств**. Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

4) **Координация и взаимодействие** внутри и вне предприятия. Меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия. Организовать координацию и взаимодействие внутри и вне предприятия может комитет (группа, совет и т.д.) безопасности предприятия.

5) **Сочетание гласности с конспирацией**. Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль - предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6) **Компетентность**. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

7) **Экономическая целесообразность**. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

8) **Плановая основа деятельности**. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и

т.д.) и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

9) **Системность**. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

1.2 Субъекты безопасности предприятия

Обеспечением безопасности предприятия занимаются две группы субъектов, которые отображены на рисунке 1.2.

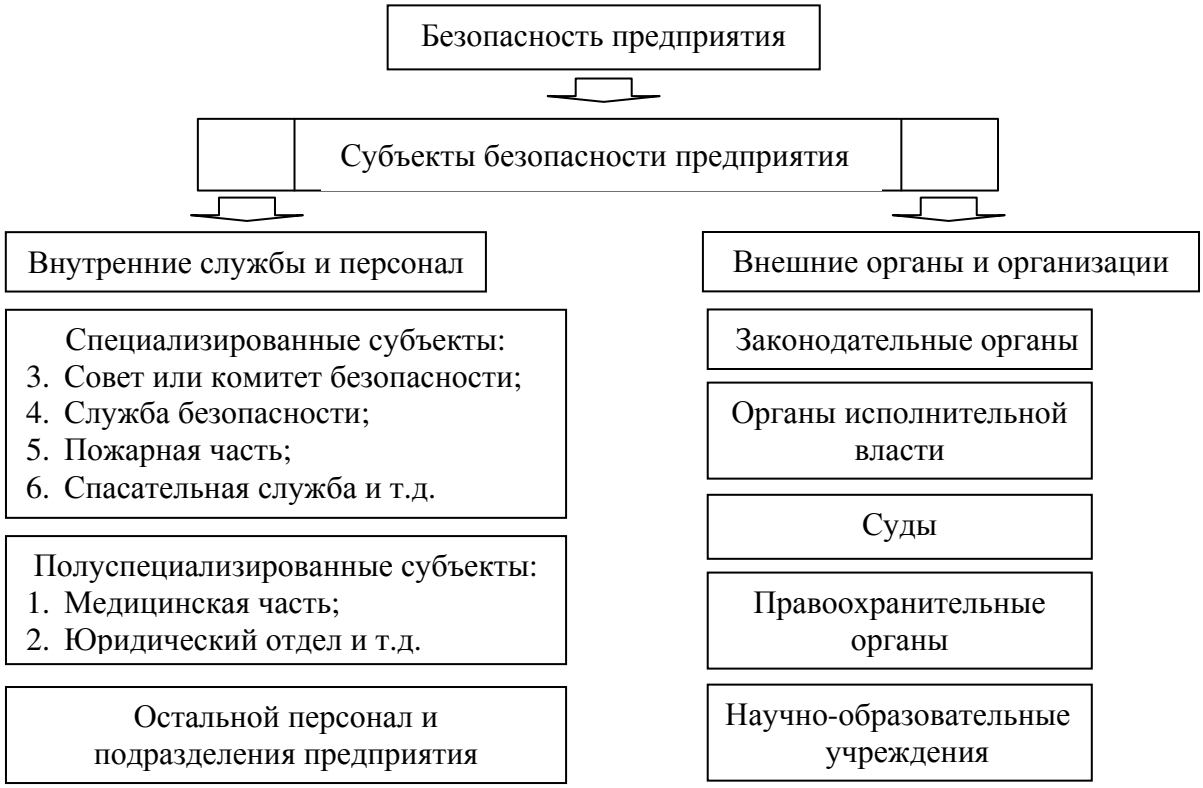

Рисунок 1.2 – Субъекты безопасности предприятия

Первая группа занимается этой деятельностью непосредственно на предприятии и подчинена его руководству. Среди этой группы можно выделить специализированные субъекты: совет или комитет безопасности предприятия, служба безопасности, пожарная часть, спасательная служба и т.д.), основным предназначением которых является постоянная профессиональная деятельность по обеспечению безопасности предприятия (в рамках своей компетенции). Другую часть субъектов этой группы условно можно назвать полуспециализированной, т.к. часть функций этих субъектов предназначена для обеспечения безопасности предприятия (медицинская часть, юридический отдел и т.д.). Наконец, к третьей части этой группы субъектов относится весь остальной персонал и подразделения предприятия, которые в рамках своих должностных инструкций и положений о подразделениях обязаны принимать меры к обеспечению безопасности.

Следует иметь в виду, что эффективно обеспечивать безопасность предприятия эти субъекты могут только в том случае, если цели, задачи, функции, права и

обязанности будут распределены между ними таким образом, чтобы они не пересекались друг с другом.

Ко второй группе субъектов относятся внешние органы и организации, которые функционируют самостоятельно и не подчиняются руководству предприятия, но при этом их деятельность оказывает существенное (положительное или отрицательное) влияние на безопасность предприятия. Субъектами этой группы являются:

1. **Законодательные органы**. Принятые на уровне Российской Федерации и субъектов Федерации законы составляют правовую основу деятельности по обеспечению безопасности предприятия.

2. **Органы исполнительной власти**. Принятые на уровне этих органов подзаконные акты во многом дополняют, уточняют, детализируют требования законов.

3. **Суды**. Судебные органы обеспечивают соблюдение законных прав и интересов предприятия, в т.ч. в сфере безопасности.

4. **Правоохранительные органы**. Такие органы осуществляют борьбу с правонарушениями, которые отрицательным образом влияют на состояние безопасности предприятия.

5. **Научно-образовательные учреждения**. Последние (особенно негосударственные образовательные учреждения для подготовки частных охранников и детективов) призваны обеспечить научно-методическую проработку проблем безопасности предприятия и подготовку соответствующих специалистов в сфере безопасности предприятий.

Совершенно очевидно, что субъекты второй группы по своей инициативе подключаются эпизодически (или никогда) к деятельности предприятия по обеспечению своей безопасности. Организационной формой такого подключения может стать комплексная программа безопасности предприятия, в которой необходимо предусмотреть формы и методы этой работы. Кроме того, можно рекомендовать разработку планов структурных подразделений и всего предприятия в целом по организации взаимодействия с вышеуказанными органами и организациями.

1.3 Средства и методы обеспечения безопасности

Среди существующих средств обеспечения безопасности можно выделить следующие:

1. **Технические средства**. К ним относятся охранно-пожарные системы, видео-, радиоаппаратура, средства обнаружения взрывных устройств, бронежилеты, заграждения и т.д.

2. **Организационные средства**. Создание специализированных орг-струкгурных формирований, обеспечивающих безопасность предприятия.

3. **Информационные средства**. Прежде всего это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Кроме этого, важнейшая информация для принятия решений по вопросам безопасности сохраняется в компьютерах.

4. **Финансовые средства**. Совершенно очевидно, что без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей.

5. **Правовые средства**. Здесь имеется ввиду использование не только изданных

вышестоящими органами власти законов и подзаконных актов, но также разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности.

6. **Кадровые средства**. Имеется ввиду прежде всего достаточность кадров, занимающихся вопросами обеспечения безопасности. Одновременно с этим решают задачи повышения их профессионального мастерства в этой сфере деятельности.

7. **Интеллектуальные средства**. Привлечение к работе высококлассных специалистов, научных работников (иногда целесообразно привлекать их со стороны) позволяет внедрять новые системы безопасности.

Следует заметить, что применение каждого из вышеуказанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе. В то же время необходимо отметить, что одновременное внедрение всех вышеуказанных средств в принципе невозможно. Оно проходит обычно ряд этапов:

I этап. Выделение финансовых средств.

II этап. Формирование кадровых и организационных средств.

III этап. Разработка системы правовых средств.

IV этап. Привлечение технических, информационных и интеллектуальных средств.

Переведенные из статичного в динамичное состояние вышеуказанные средства становятся методами, т.е. приемами, способами действия. Соответственно, можно говорить о технических, организационных, информационных, финансовых, правовых, кадровых и интеллектуальных методах.

1.4 Проектирование системы безопасности

Для начала рассмотрим основной принцип функционирования коммерческих организаций на основе обобщенной модели (Рисунок 1.3). С точки зрения данного подхода, особое значение приобретает учет руководителем всей совокупности интересов организации.

В этой модели центральный блок представляет собой саму организацию (Рисунок 1.4) со своими непосредственными видами коммерческой деятельности.

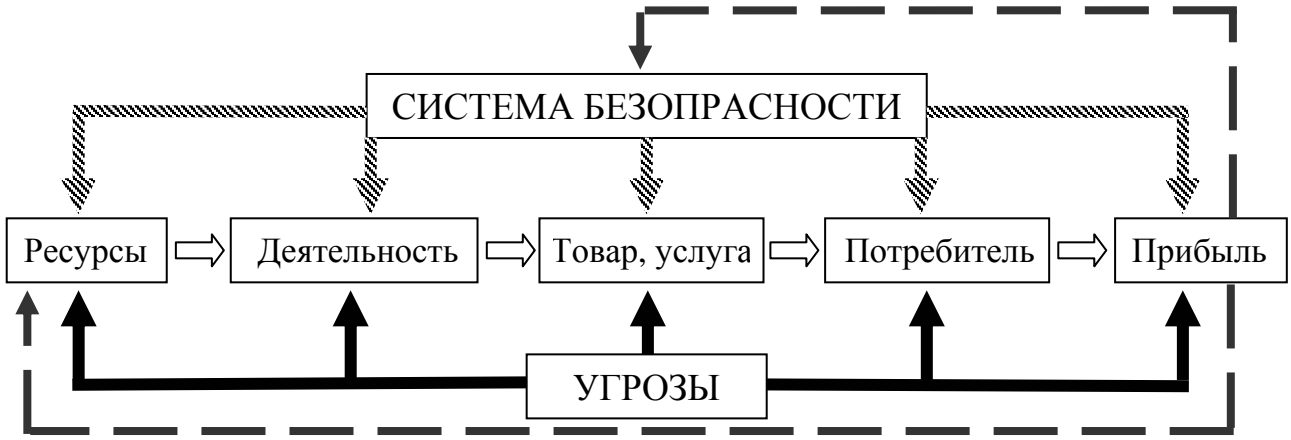

Рисунок 1.3 – Обобщенная модель функционирования коммерческой организации

На выходе системы - получаемая прибыль, стабильное положение на рынке и авторитет организации.

Управляемыми входами на трех этапах (предотвращение, пресечение, ликвидация последствий) несанкционированных входных воздействий (НСВВ) на организацию, как систему являются: служба безопасности, организационные мероприятия и технические средства, входящие в состав ИСБ. Причем технические средства безопасности обеспечивают усиление функционирования системы безопасности и служат общим целям предупреждения и противодействия угрозам, воздействующим на объекты защиты предпринимательской деятельности.

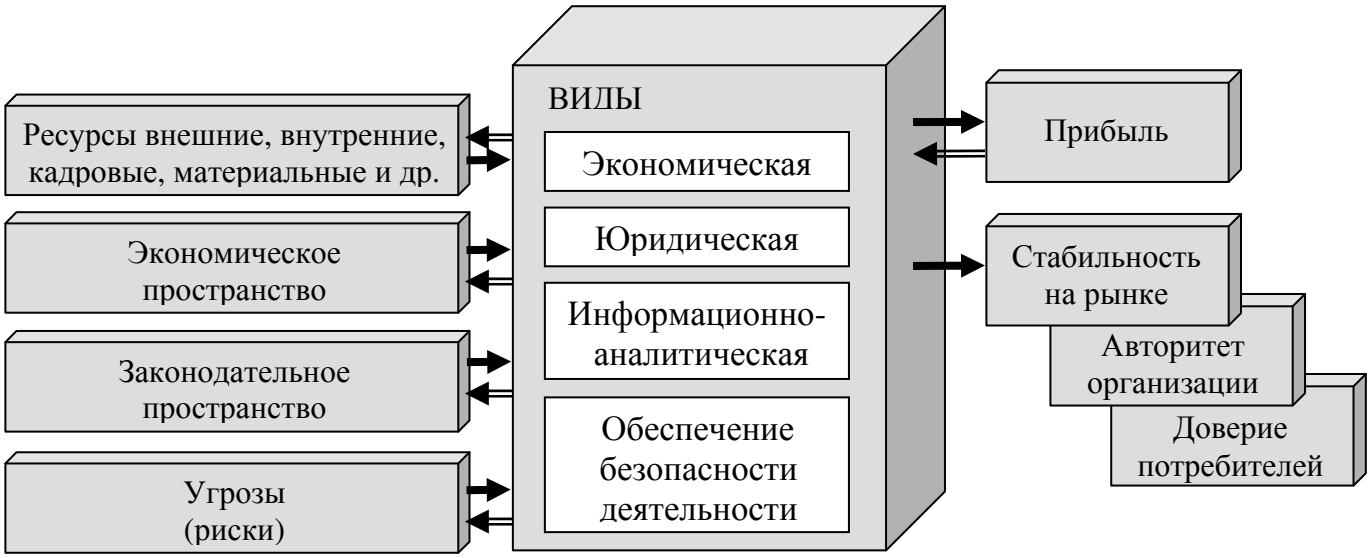

Рисунок 1.4 – Обобщенная схема получения прибыли коммерческой организацией

Рассмотренная нами обобщенная модель функционирования коммерческих организаций показывает, что система безопасности предпринимательской деятельности непосредственно оказывает существенное влияние на деятельность всей организации, а также позволяет увеличить ее доход за счет снижения рисков. Чтобы успешно управлять системой безопасности, ее руководители должны быть компетентны в вопросах обеспечения безопасности, так как от этого, прежде всего, зависят как состояние защищенности предпринимательских структур, так и их личная безопасность.

В данном контексте необходимо рассматривать систему безопасности в широком смысле, то есть как систему, обеспечивающую не только безопасность бизнеса, но и помогающую его оптимизировать и развивать. Под возможностью развития бизнеса средствами системы безопасности нужно понимать следующее:

1. Оптимизируя саму систему безопасности, мы минимизируем издержки на безопасность, следовательно, мы уже увеличиваем доход организации.

2. Криминальный бизнес не входит в существующее законодательное пространство, а одной из основных функций системы безопасности является обеспечение юридической безопасности деятельности, то есть законное оформление договоров, счетов, ценных бумаг и т.п. В противном случае организация может попасть под влияние организованной преступности. Организация рискует понести значительные убытки, потерять авторитет, стабильность на рынке, а также может прекратить свое существование. Поэтому одна из главных задач системы безопасности - это не дать организации уйти в область незаконного (криминального)

бизнеса, где область рисков расширяется по экспоненциальной зависимости.

3. Экономическая безопасность должна обеспечиваться силами и средствами экономической и финансовой служб организации.

4. Контроль за правильным расходом и распределением ресурсов. Обеспечение надежности сотрудников позволяет предотвратить возможность "работы" на конкурентов.

5. Предупреждение, предотвращение максимального количества угроз и ликвидация их последствий - являются главной задачей системы безопасности.

1.5 Концепция безопасности

Зарубежный и отечественный опыт обеспечения безопасности свидетельствуют, что для борьбы со всей совокупностью потенциально возможных угроз необходима стройная и целенаправленная организация процесса противодействия. Причем в организации этого процесса должны участвовать не только люди ответственные за это направление, а также: профессиональные специалисты, руководство организации, ведущие сотрудники организации. Для этого необходимо разрабатывать под каждую конкретную организацию свою концепцию безопасности.

Концепция безопасности организации выражает систему взглядов на проблему безопасности на различных этапах и уровнях предпринимательской деятельности, а также основные принципы, направления и этапы реализации мер безопасности.

При построении концепции безопасности руководитель организации и начальник службы безопасности должны очень тщательно анализировать полный набор угроз, глубокое знание и своевременное выявление которых позволит службе безопасности превентивно их блокировать. Накопленный в мире опыт в области безопасности показывает, что:

- анализ угроз и разработка концепции безопасности не должны быть одноразовыми актами. Это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее слабых мест и ликвидации недостатков;
- безопасность может быть обеспечена лишь при комплексном использовании всего арсенала сил и средств во всех структурных элементах системы, то есть использования ИСБ;
- никакая ИСБ не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала организации и пользователей и соблюдения ими всех установленных правил, направленных на обеспечение безопасности;
- основной целью системы безопасности является предупреждение.

Безопасность деятельности организации осуществляется на двух уровнях:

1. Всеми сотрудниками организации посредством выполнения режима безопасности;
2. Службой безопасности организации путем проведения защитных мероприятий.

1.6 Создание и ликвидация службы безопасности предприятия

Правовой статус охранно-сыскного подразделения или службы безопасности предприятия имеет ряд особенностей, которые выделяют его из других форм частной детективной и охранной деятельности. Знание этих особенностей имеет не только научное, но и практическое значение.

Прежде всего, обращает на себя внимание особый порядок создания и ликвидации службы безопасности.

Под предприятием, которое вправе учреждать собственную службу безопасности, понимается исключительно коммерческая организация (полное товарищество, товарищество на вере, общество с ограниченной ответственностью, общество с дополнительной ответственностью, акционерное общество, производственный кооператив, государственное унитарное предприятие и муниципальное унитарное предприятие).

Предприятие-учредитель представляет в органы внутренних дел (по месту своего нахождения) следующие документы:

- заявление о согласовании Устава службы безопасности;
- Устав службы безопасности;
- лицензии на руководителя и персонал службы безопасности;
- сведения о характере и направлениях деятельности службы безопасности, составе и предполагаемой численности персонала, наличии специальных средств, технических и иных средств, а также потребности в них и оружии.

Учредителями службы безопасности не могут быть физические лица (даже имеющие лицензии на осуществление частной детективной и охранной деятельности) или несколько юридических лиц.

При создании службы безопасности предприятие-учредитель может предоставить ей право открывать текущий и расчетный счета в банке (это должно найти отражение в Уставе). Текущий счет предназначен только для операций, связанных с выдачей наличных денег, а по расчетному счету проводятся операции, связанные с безналичными перечислениями.

Ликвидация службы безопасности может произойти при добровольном отказе его персонала от выполнения своих обязанностей, по инициативе предприятия-учредителя, при ликвидации предприятия-учредителя и в случае аннулирования органом внутренних дел лицензии всем охранникам и детективам.

Важнейшей особенностью любой службы безопасности является обязательное наличие в ее структуре как детективных, так и охранных подразделений. Безусловно, такое сочетание позволяет наладить взаимодействие между ними, проводить комплексные мероприятия по предупреждению и пресечению правонарушений и т.д., что, в конечном счете, повышает эффективность деятельности службы безопасности.

Несмотря на отсутствие единых правил, можно рекомендовать при определении соотношения детективных и охранных подразделений внутри службы безопасности использовать следующие критерии:

- наличие коммерческой тайны;
- состояние, структура и динамика правонарушений на предприятии;
- наличие значительных материальных ценностей, и валюты;
- реальная и потенциальная сумма нанесенного предприятию ущерба;
- имеющиеся факты промышленного шпионажа;
- реальность угроз физической расправы над сотрудниками предприятия со стороны преступных элементов;
- фактические возможности со стороны местных правоохранительных органов в оказании помощи предприятию в пресечении правонарушений;
- взаимоотношения с конкурентами и соблюдение правил функционирования

рыночной экономики;

• степень правовой и иной подготовки сотрудников по вопросам обеспечения безопасности предприятия и т.д.

Служба безопасности предназначена, прежде всего, для организации защиты от всех видов угроз.

Детализация тех угроз, устранение, пресечение или нейтрализация которых входит в компетенцию службы безопасности, должна найти отражение в ее уставе применительно к основным видам безопасности. Приведем краткий перечень возможных действий службы безопасности по пресечению, устранению или нейтрализации угроз в рамках основных видов безопасности (Рисунок 1.5).

Рисунок 1.5 – Основные виды безопасности предприятия

1. **Физическая безопасность** - охрана персонала от насильственных преступлений, предупреждение таких преступлений и т.д.

2. **Информационная безопасность** - сохранение коммерческой тайны, борьба с хакерами и т.д.

3. **Экономическая безопасность** - охрана имущества предприятия, борьба с экономическим шпионажем и т.д.

4. **Экологическая безопасность** - документирование экологических правонарушений, выставление экологических постов и т.д.

5. **Пожарная безопасность** - проектирование, монтаж и эксплуатационное обслуживание пожарной сигнализации, выставление постов в местах возможного загорания и пожаров и т.д.

6. **Техногенная безопасность** - охрана наиболее опасных участков предприятия от террористов, участие в расследовании техногенных катастроф и т.д.

7. **Психологическая безопасность** - информирование персонала предприятия об отсутствии реальных угроз, адекватное реагирование на дезинформационные мероприятия и т.д.

8. **Научно-техническая безопасность** - охрана ноу-хау, организация охраны научных лабораторий и т.д.

Саму же **службу безопасности**, призванную обеспечить безопасность предприятия, можно определить как его структурное формирование, осуществляющее в рамках законодательства и собственного устава меры по предотвращению и пресечению угроз интересам своего учредителя.

Под **Уставом** понимается правовой акт, определяющий свод правил, регулирующих деятельность организации, её взаимоотношения с другими

организациями и гражданами, права и обязанности в определенной сфере её деятельности.

Сложность в разработке устава заключается в том, что в нем должны быть изложены в краткой, но емкой форме, основы жизнедеятельности службы безопасности. Прежде всего, в него целесообразно включить следующие разделы:

1. Общие положения;
2. Основные задачи, функции;
3. Права и обязанности;
4. Руководство;
5. Взаимоотношения и связи;
6. Охрана и детективная деятельность;
7. Имущество и средства;
8. Контроль;
9. Проверка и ревизия деятельности;
10. Реорганизация и ликвидация.

1.7 Основные функции службы безопасности

Как правило выделяют следующие функции службы безопасности:

1. Реализация мер противодействия всех видов шпионажа (промышленного, научно-технического, экономического и т.д.);
2. Своевременное информирование руководства предприятия о фактах нарушения законодательства со стороны государственных и муниципальных органов, коммерческих и некоммерческих организаций, затрагивающих интересы предприятия;
3. Предупреждение переманивания сотрудников предприятия, обладающих конфиденциальной информацией;
4. Всестороннее изучение деловых партнеров;
5. Своевременное выявление и адекватное реагирование на дезинформационные мероприятия;
6. Разработка и совершенствование локальных правовых актов, направленных на обеспечение безопасности предприятия;
7. Реализация мер по защите коммерческой и иной информации;
8. Организация мероприятий по противодействию недобросовестной конкуренции;
9. Обеспечение защиты всех видов ресурсов предприятия;
10. Реализация мер по защите интеллектуальной собственности;
11. Организация и проведение мер по предотвращению чрезвычайных ситуаций;
12. Выявление негативных тенденций среди персонала предприятия, информирование о них руководства предприятия и разработка соответствующих рекомендаций;
13. Организация взаимодействия с правоохранительными и контрольными органами в целях предупреждения и пресечения правонарушений, направленных против интересов предприятия;
14. Разработка и реализация мер по предупреждению угроз физической безопасности имуществу предприятия и его персоналу;

15. Возмещение материального и морального ущерба, нанесенного предприятию в результате неправомерных действий организаций и отдельных физических лиц.

1.8 Роль руководства службы безопасности предприятия

Служба безопасности фирмы, предприятия, банка в лице ее начальника подчиняется непосредственно первому лицу предприятия. Прерогативой руководителя фирмы, предприятия по обеспечению безопасности руководимой им структуры является решение следующих вопросов:

1. Разработка стратегии деятельности службы безопасности;
2. Указание основных направлений в обеспечении безопасности предприятия;
3. Утверждение нормативных актов, разработанных службой безопасности;
4. Дача распоряжений начальнику службы безопасности по разработке аналитических документов, связанных с исследованием различных аспектов обеспечения безопасности предприятия;
5. Издание на основе анализа этих документов соответствующих распоряжений по совершенствованию обеспечения безопасности предприятия;
6. Привлечение начальника службы безопасности к ведению деловых переговоров с солидными клиентами, потенциальными партнерами и их изучение;
7. Привлечение службы безопасности к участию в подборе сотрудников предприятия;
8. Дача распоряжений по использованию службы безопасности в процессе обучения персонала предприятия по вопросам безопасности;
9. Утверждение структуры службы безопасности;
10. Выделение финансовых средств для деятельности службы безопасности;
11. Организация совета безопасности предприятия под руководством первого лица банка, фирмы, предприятия;
12. Создание механизма управления предприятием в чрезвычайных ситуациях;
13. Оценка эффективности деятельности службы безопасности и др.

Первое лицо предприятия в своей деятельности должно руководствоваться рядом аксиом: «Безопасность - это наука, которую надо изучать и развивать, это искусство, которое надо постигать, это культура, которую надо воспитывать у бизнесмена»; «Опасность легче упредить, чем с ней бороться» и др. Предпринимателю необходимо подобрать такого начальника службы безопасности своего предприятия, которому можно доверять; он должен быть заместителем первого лица по безопасности предприятия. Умелое руководство службой безопасности, использование грамотно разработанных систем и программ предупреждения угроз и преступлений позволяет получить прямой материальный выигрыш. Управление деятельностью службы безопасности первым лицом должно быть таким, чтобы все ее сотрудники стремились следовать принципу «преданность фирме». От этого во многом зависит стабильность предпринимательских структур и достижение ими своих целей.

В настоящее время в России созданы десятки тысяч фирм и иных коммерческих организаций. Примерно 50% из них решают проблему безопасности путем создания собственных служб безопасности или привлечения частных детективно-охранных структур. Зарубежный опыт обеспечения безопасности

предпринимательской деятельности свидетельствует о том, что предпочтительным является вариант создания предприятием своего подразделения, обеспечивающего безопасность. Но далеко не каждая коммерческая структура в состоянии создать собственную службу безопасности, да порой в этом и нет необходимости. В подобных случаях бизнесмены заключают соглашения с частными детективно-охранными структурами. Однако, прежде чем пойти на такой шаг, следует непременно изучить детективно-охранную фирму с точки зрения продолжительности ее деятельности, круга клиентов, профессионального уровня, надежности, кадрового состава, финансового положения.

1.9 Принципы формирования службы безопасности предприятия

С учетом характера и масштабов деятельности организации, анализа потенциальных и реальных угроз их безопасности со стороны криминальных элементов и конкурентов, а также финансовых возможностей руководство организации определяет структуру и численность службы безопасности.

Служба безопасности крупного предприятия состоит, как правило, из следующих основных подразделений (Рисунок 1.6):

Информационно-аналитический отдел.

- оптимизация деятельности службы безопасности;
- минимизация рисков и максимизация прибыли.

Участвует в разработке концепции безопасности организации и проектировании интегрированной системы безопасности. Должен работать непрерывно, отслеживая изменение параметров системы. Разрабатывает оперативно-тактические планы.

Отдел собственной безопасности.

- контроль персонала;
- проверка деятельности персонала по обеспечению безопасности;
- усиление исполнительской дисциплины;
- взаимодействие с правоохранительными органами.

Подсистема функционирует на основе принципов объективности, систематичности, своевременности, конкретности, целенаправленности. Используемые методы: наблюдение, обследование, эксперимент. По результатам контрольно-проверочных мероприятий разрабатываются конкретные предложения по устранению имеющихся недостатков и оказанию практической помощи исполнителям в совершенствовании работы.

Отдел обеспечения режима и физической охраны.

- обеспечение сохранности материальных ценностей;
- обеспечение сохранности физических носителей информации;
- обеспечение сохранности персонала.

Инженерно-технический отдел.

- на основе концепции безопасности должен обеспечить оптимальное распределение технических средств по всей структуре службы безопасности;
- контроль работы и своевременное обновление и внедрение парка новых технических средств.

За счет этого достигается минимизация людских и иных ресурсов в процессе обеспечения безопасности, а также обеспечивается максимальная надежность охраны, минимальные затраты на эксплуатацию.

Отдел экономической и информационной безопасности.

- обеспечение безопасности экономической деятельности организации;

- защита ее коммерческой тайны.

Осуществляет получение дополнительной информации об экономическом пространстве и его изменении законными путями. Обеспечивает защиту от промышленного шпионажа, недобросовестной конкуренции, разведывательных мероприятий других организаций. Осуществляет взаимодействие со средствами массовой информации.

Юрист-эксперт, юрист-консультант.

- детальный анализ всех документов, подлежащих утверждению руководителями организации;
- контроль документооборота;
- экспертиза договоров.

Своевременный учет изменения законодательства для того, чтобы не уйти в сферу криминального бизнеса, исключение экономических потерь, ликвидации организации, штрафных санкций, юридических исков и т.п.

Оперативный совет безопасности.

- является консультационным органом службы безопасности и служит для разрешения спорных и сложных вопросов в осуществлении деятельности службы безопасности.

В этот совет входят руководитель организации и ведущие специалисты из всех подразделений службы безопасности, председателем является, как правило, руководитель организации.

Кризисная группа.

- противодействие внезапно возникающим критическим (кризисным) ситуациям,
- оценка обстановки,
- принятие неотложных мер по безопасности,
- управление деятельностью фирмы в экстренных условиях,
- обеспечение оперативного взаимодействия с органами правопорядка.

Она создается из числа ключевых фигур организации: руководителя, начальников подразделений, филиалов, служб, юриста, главного бухгалтера и др. В каждом конкретном случае в состав кризисной группы могут включаться те или иные специалисты. Рабочие заседания группы должны проходить в условиях предельной конфиденциальности.

На практике также широко распространена следующая структура службы безопасности крупного предприятия, которая состоит, как правило, из следующих подразделений:

1. Оперативного.
2. Добывания коммерческой информации.
3. Информационно-аналитического.
4. Режима и охраны.
5. Защиты электронно-вычислительной техники и каналов связи.

Основные функции **оперативного подразделения**:

- обеспечение безопасности руководства, главных специалистов и других сотрудников предприятия;
- обеспечение безопасности объектов, территории, оборудования и продукции фирмы;
- контроль за соблюдением действующих на предприятии режимов;

Рисунок 1.6

- выявление факторов подготовки различных акций в отношении предприятия, их сотрудников и клиентов со стороны криминальных элементов и конкурентов;
- противодействие этим акциям;
- контроль за обстановкой в коллективах подразделений предприятия;
- сбор и представление в информационно-аналитическое подразделение службы безопасности данных о фактах, имеющих значение для обеспечения безопасности предприятия;
- связь со средствами массовой информации;
- контроль за научными и иными публикациями сотрудников предприятия.

Основные функции **подразделения добывания коммерческой информации** сводятся к получению следующих сведений:

- о криминальных элементах в местах и районах расположения предприятия и проживания их руководителей и персонала;
- о конкурентах предприятия и потенциальных клиентах;
- о конъюнктуре рынка в соответствующих регионах и странах;
- об обстановке в тех регионах и странах, где предприятие, фирма планируют выйти на рынок.

Подразделение службы безопасности также занимается постоянным изучением партнеров и клиентов, с которыми заключены кредитные и иные договоры на крупные суммы, и проводит мероприятия по созданию благоприятных условий для выхода предприятия на рынок. Вся добытая информация представляется в информационно-аналитическое подразделение службы безопасности.

Основные функции **информационно-аналитического подразделения**:

- сбор информации по вопросам обеспечения безопасности предприятия от подразделений службы безопасности;
- переработка этой информации в соответствии с разработанной и заложенной в информационную систему структурой;
- выдача имеющейся в базе данных информации по требованию руководства предприятия и службы безопасности;
- исследование поступающей в базу данных информации и представление первому лицу предприятия аналитических обзоров и иных документов;
- защита базы данных от умышленного или неумышленного разрушения и утечки накопленной в ней информации к криминальным элементам и конкурентам;
- организация координации и взаимодействия с другими базами данных предприятия и с разрешения их руководства - с банками данных партнеров и информационных центров.

Основные функции **подразделения режима и охраны**:

- разработка и реализация режимов физической охраны (руководства предприятия и некоторых главных специалистов, персонала и клиентов, объектов, территории, оборудования, продукции, перевозок финансовых средств, сырья, продукции);
- контроль за выполнением сотрудниками установленных на предприятии режимов;
- физическое противодействие возможным акциям криминальных элементов и конкурентов в отношении руководства, персонала, клиентов, объектов, наличности;

- взаимодействие с государственными правоохранительными органами в вопросах обеспечения физической безопасности предприятия;
- сбор и предоставление в информационно-аналитическое подразделение сведение о фактах, имеющих значение для обеспечения безопасности предприятия.

Основные функции **подразделения защиты электронно-вычислительной техники и каналов связи**:

- выявление технических каналов утечки конфиденциальной информации и возможных фактов ведения криминальными элементами и конкурентами технической разведки против предприятия;
- предотвращение утечки конфиденциальной информации посредством технических средств и каналов;
- применение технических средств для добывания сведений о конкурентах и др.;
- предоставление в информационно-аналитическое подразделение информации о выявленных угрозах безопасности предприятия со стороны криминальных элементов и конкурентов с использованием технических средств.

Для оптимального функционирования системы безопасности необходимо, во-первых обеспечить эффективное построение организационно-штатной структуры службы безопасности организации, а затем на основе математических методов осуществить проектирование ИСБ. Наиболее приемлемым способом решения первой проблемы является использование автоматизированных средств проектирования организационно-штатных структур. Такая система может состоять из нескольких модулей обеспечивающих сбор, оценку и обработку экспертной и статистической информации.

Центральным звеном в системе подобного рода будет программный модуль синтеза и оптимизации организационно-штатных структур. Основной принцип работы этого модуля - оптимизация ориентированного графа. Следующим этапом является формирование нормативной базы и разработка должностных инструкций для сотрудников службы безопасности. На основе выявленных угроз, руководитель организации совместно с начальником службы безопасности с использованием прогнозов информационно-аналитического отдела может практически полностью решить вопросы концептуального управления службой безопасности и проектирования ИСБ. Для этого необходимо с помощью экспертной группы, в состав которой входят руководители и специалисты подразделений служб безопасности организации, правильно оценить принципы функционирования организации. При этом необходимо с точки зрения безопасности коммерческой деятельности организации ответить на следующие вопросы: Что производить? Для кого производить? Каким образом производить? Как получить максимальную прибыль, обеспечивая при этом безопасность своей деятельности? Также необходимо провести тщательное обследование помещений организации с целью выявления наиболее уязвимых зон. Производится анализ путей прохождения и порядок хранения материальных ценностей, расположение компьютерных линий связи и информационных потоков, места и способы хранения рабочей и архивной информации, расположение телефонных линий связи, электрических, водопроводных, вентиляционных и других инженерных коммуникаций. Такое обследование позволит моделировать возможное поведение злоумышленника и сценарий его предполагаемых действий.

Основным итогом обследования на этом этапе должно стать определение зон защиты и установление степеней их значимости. На практике **зонами защиты** может быть часть территории, отдельное здание, а также места для приема посетителей, автотранспорт, каналы связи, вычислительный комплекс и т.д. Когда сформирована концепция безопасности организации, важно определить возможные силы и средства для построения системы безопасности. В первую очередь рассматриваются кадровые ресурсы для формирования структуры службы безопасности. При противодействии НСВВ они играют основную роль, обеспечивая охрану, проводя профилактические мероприятия, организовывая и поддерживая заданный режим работы организации. Помимо определения состава организационно-штатной структуры и расстановки кадров, необходимо наметить набор технических средств, которые будут использованы при построении ИСБ. Технические средства оказывают существенную помощь сотрудникам службы безопасности для выполнения функций безопасности организации. С их использованием происходит блокирование угроз, автоматический контроль целостности границ зон защиты, ведется дистанционный визуальный контроль, оперативно изменяется степень защищенности охраняемых зон. Кроме того, автоматически протоколируются все факты попыток реализации НСВВ, а в случае их успешной реализации фиксируются события и действия службы безопасности по их пресечению и ликвидации последствий. Приоритетными для выполнения являются требования обеспечивающие ликвидацию угроз, приводящих к максимально возможному ущербу. Технические средства управления и контроля функционирования совместно действующих подсистем должны определяться их целевой функцией. Предпочтительны автоматические средства управления и контроля, но как дублирующие допускаются и ручные. Целесообразность дублирования определяется требованиями обеспечения эксплуатационной надежности систем. Средства управления и контроля должны иметь защиту от возможных ошибочных действий персонала, а также от несанкционированного доступа к линиям передачи сигналов управления.

На основе проведенного анализа российской практики обеспечения безопасности деятельности предприятия можно сделать следующие выводы.

1. Для проектирования оптимальной системы безопасности предпринимательской деятельности необходимо иметь четкое представление о функционировании конкретной коммерческой организации, для которой проектируется система.
2. Система безопасности, вопреки обобщенной точке зрения о дополнительных затратах, непосредственно оказывает положительное влияние на деятельность всей организации, а также позволяет увеличить ее доход.
3. Для оптимального функционирования службы безопасности организации необходимо: обеспечить проектирование эффективной организационно-штатной структуры, грамотное формирование нормативной базы и должностных обязанностей, а также оптимальное распределение технических средств безопасности по сотрудникам.
4. Приведена обобщенная классификация технических средств безопасности, входящих в состав ИСБ и находящихся на вооружении сотрудников служб безопасности.

1.10 Технология защиты от угроз экономической безопасности

Практическая деятельность службы экономической безопасности должна основываться на использовании типовых схем, процедур и действий. Прежде всего, следует сказать об общем алгоритме действий, на котором основана работа службы безопасности.

Система предупредительных мер включает деятельность по изучению контрагентов, анализ условий договоров, соблюдение правил работы с конфиденциальной информацией, защита компьютерных систем и т.д. Эта деятельность осуществляется регулярно и непрерывно. Она обеспечивает защиту экономической безопасности на основе постоянно действующей системе организационных мероприятий.

Однако даже самая лучшая система предупредительных мер не может предвидеть, а тем более преодолеть внезапно возникающие нестандартные угрозы, которые могу причинить значительный ущерб фирме, например мошеннического характера. Для противодействия этим угрозам необходимо применять специфический механизм. Американские специалисты в области выявления, расследования и предупреждения мошенничества, предлагают использовать активную модель реагирования при обнаружении мошенничества.

Отличительной особенностью этой оригинальной модели является во-первых, то, что она предусматривает обязательное реагирование на каждый случай на каждый случай мошеннических угроз, и, во-вторых, включает такие блоки, которые повышают эффективность работы службы экономической безопасности. К ним относятся, например:

1. “**Сообщения о случившемся**” – он подразумевает, что среди персонала фирмы необходимо создать такой климат, который позволяет облегчить людям возможности для сообщения о подозрениях или фактах;
2. “**Огласка**” - предполагает распространение информации о способах совершения мошенничества, лицах, их совершивших, среди руководства, работников службы безопасности, других фирм;
3. “**Профессиональная подготовка**” предполагает постоянное повышение квалификации менеджеров, аудиторов, работников службы безопасности.

В то же самое время, какую бы модель обеспечения экономической безопасности ни выбрал предприниматель (руководитель фирмы), следует учитывать тот факт, что организация эффективной системы профилактических, предупредительных мер обойдется гораздо дешевле, чем борьба с последствиями уже случившихся правонарушений, реализованных угроз.

Вопросы для повторения темы:

1. Что следует понимать под безопасностью объекта?
2. Перечислите основные функции безопасности по отношению к угрозам.
3. На основе каких принципов строится система безопасности предприятия?
4. Что Вы понимаете под возможностью развития бизнеса средствами системы безопасности?
5. Предприятие, какой формы собственности вправе учреждать собственную службу безопасности? Какие документы оно должно предоставить в органы внутренних дел?

6. Могул ли физические лица быть учредителями службы безопасности?
7. Перечислите существующие способы ликвидации службы безопасности.
8. Какие разделы включаются в Устав службы безопасности?
9. На основе каких принципов функционирует отдел собственной безопасности?
10. Кто вправе входить в оперативный совет безопасности?
11. Что включает в себя система предупредительных мер по защите от угроз экономической безопасности предприятия? В чем ее основной недостаток?
12. Из каких основных блоков состоит активная модель реагирования?

Литература:

1. Грунин О.А. Экономическая безопасность организации. - М.: ИНФРА-М, 2002. - 267с.
2. Доронин А.И. Бизнес разведка. - М.: Ось-89, 2002. - 288с.
3. Землянов В.М. Своя контрразведка. - Минск: Харвест, 2002. - 416с.
4. Корж П., Клопов И. Негосударственная безопасность. - Ростов-на-Дону: Феникс, 2002. - 448с.
5. Экономическая безопасность хозяйственных систем /Под, ред. А.В. Колосова- М.: Издательство РАГС, 2001. - 446с.

Глава 2. Обеспечение экономической безопасности предприятия при работе с персоналом

Ключевые понятия:
Личностные опросные листы
Бланковые методики
Проективные методики
Приборные методики

2.1 Общие положения

Практика последнего времени свидетельствует о том, что различные по масштабам, последствиям и значимости виды преступлений и правонарушений так или иначе связаны с конкретными действиями сотрудников данного предприятия. В связи с этим представляется целесообразным и необходимым в целях повышения экономической безопасности этих объектов уделять больше внимания подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи. При этом необходимо также в обязательном порядке проводить значительную разъяснительно-воспитательную работу, систематические инструктажи и учения по правилам и мерам безопасности, регулярные, но неожиданные тестирования различных категорий сотрудников по постоянно обновляемым программам.

Следует в трудовых контрактах четко описывать персональные функциональные обязанности всех категорий сотрудников предприятий и на основе существующего российского законодательства во внутренних приказах и распоряжениях определять их ответственность за любые виды нарушений,

связанных с разглашением или утечкой информации, составляющей коммерческую тайну или имеющей конфиденциальный характер.

Кроме того, в этой связи целесообразно отметить, что многие предприятия все шире вводят в своих служебных документах гриф «конфиденциально» и распространяют различного рода надбавки к окладам для соответствующих категорий своего персонала.

Постепенно приобретают все большую значимость при приёме на работу рекомендательные письма, научные методы проверки на профпригодность и различного рода тестирование, осуществляемое соответствующими службами.

2.2 Психологический подход к отбору сотрудников

Если объективно оценивать существующие сегодня процедуры отбора персонала, то окажется, что во многих организациях основное внимание, к сожалению, делается прежде всего на выяснении лишь уровня профессиональной подготовки кандидатов на работу, который определяется зачастую по традиционно-формальным признакам: образование; разряд; стаж работы по специальности. Это соответствует все более устаревающей концепции ограниченной материально-финансовой ответственности отдельных работников за конечные результаты своей деятельности и сохранность конфиденциальной информации.

В современных же динамично развивающихся структурах при стремлении к весьма ограниченной численности сотрудников, все более частом совмещении рядовыми исполнителями различных участков работы и стремительно увеличивающихся потоках информации и управленческих команд, каждый сотрудник во все возрастающей степени становится носителем конфиденциальных сведений, которые могут представлять интерес как для конкурентов, так и криминальных сообществ.

В таких условиях весьма существенно повышаются и изменяются требования к личным и деловым качествам сотрудников и, следовательно, к кандидатам на работу. Данное обстоятельство побуждает руководителей все чаще обращаться к методам и процедурам научной психологии, с помощью которых можно достаточно быстро, надежно и всесторонне оценивать возможного кандидата и составлять его психологический портрет.

Однако, следует отметить, что только при умелом сочетании психологических и традиционных кадровых методов можно с высокой степенью достоверности прогнозировать поведение сотрудников в различных, в том числе экстремальных, ситуациях.

С точки зрения экономической безопасности психологический профотбор преследует следующие цели:

- выявление ранее имевших место судимостей, преступных связей, криминальных наклонностей;
- определение характера преступных склонностей, предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков в случае формирования в его окружении определенных обстоятельств;
- установление фактов, свидетельствующих о морально-психологической и эмоциональной ненадежности, неустойчивости, ущербности, уязвимости кандидата

на работу.

2.3 Организация отбора персонала

Всё чаще на предприятиях используются методики составления орг. схем или организационных чертежей, на которых графически изображается каждое рабочее место, прописываются должностные обязанности и определяются информационные потоки для отдельного исполнителя.

При такой схеме управления и контроля предельно ясно, на каком участке требуется специалист соответствующей кваллификации. Внутренними распоряжениями также определяются требования к деловым и личным качествам сотрудников и обусловливаются режимы сохранения ими коммерческой тайны.

Кроме того, при таких процедурах на каждое рабочее место рекомендуется составлять психограмму (психологический профиль специалиста), т.е. перечень личностных качеств, которыми в идеале должен обладать потенциальный сотрудник.

Обязательными атрибутами подобных документов являются разделы, отражающие профессионально важные качества, а также личностные особенности, которые делают невозможным зачисление кандидата на конкретную должность. В некоторых случаях необходимо не только указывать профессионально значимые качества, но и оценивать степень их выраженности. Как правило, проблема отбора кадров встает перед руководителями в двух основных случаях: создание новых подразделений, замещение вакантных должностей. Для первого случая характерно, как правило, изучение значительного числа кандидатур, для которых из набора имеющихся вакансий подбирается соответствующая должность. Во втором случае из ограниченного числа кандидатов отбирается тот, который по своим личным и профессиональным качествам в наибольшей степени соответствует требованиям психограммы данной должности.

2.3.1 Первый этап: предварительное собеседование

В этой фазе осуществляется предварительная беседа, которая реализуется в нескольких вариантах и может носить как относительно поверхностный, так и весьма углубленный характер. В первом случае в основном ограничиваются уточнением отдельных, наиболее значимых сведений и постановкой нескольких, совершенно конкретных вопросов. Такое собеседование проводится как правило, в случаях массового отбора кандидатов.

При углубленном же собеседовании выясняется более широкий круг вопросов, в первую очередь уточняются некоторые личностные особенности, мотивация перехода кандидата на работу именно в данное предприятие.

В последнее время выявлена также тенденция использовать ознакомительные беседы с лицами, принимаемыми на работу, для добывания через них дополнительной информации о соответствующем рынке, конкурентах, их руководстве, организационных структурах и финансовых возможностях. Таким образом, налицо стремление сотрудников некоторых кадровых подразделений придавать подобным беседам разведывательный характер, по результатам которых в ряде случаев оформляются даже отдельные информационные справки на те организации, в которых ранее работал или продолжает трудиться кандидат.

При этом, однако, кадровым службам следует помнить и о том, что не исключена вероятность провокации со стороны кандидата, который, принимая участие в подобного рода беседе, может затем официально заявить, например, через средства массовой информации, о попытках якобы выведывания у него строго охраняемых коммерческих секретов его компании.

Поэтому задача сотрудников кадровых подразделений и служб безопасности состоит в том, чтобы вести себя достаточно искренне и доброжелательно и только этим побуждать собеседника к откровенным высказываниям, что в значительной степени предотвратит впоследствии возможные обвинения в неправомерном выведывании чужих коммерческих секретов.

2.3.2 Второй этап: оценка информации о кандидатах

На этой стадии формируется первичная, но достаточно углубленная оценка личных и деловых качеств кандидата на работу. При этом для служб безопасности представляется наиболее важным добывание сведений установочно-биографического характера не только на конкретное проверяемое лицо, но и его родственников, а также выявление дружеских и особенно конфиденциальных служебных и родственных связей, скрываемых порой кандидатом от окружения, или подлинный характер которых искусственно маскируется какими-либо официальными поводами и причинами. Подобный подход позволяет резко повысить режим безопасности предприятия, но только при условии регулярности и тщательности последующих проверок.

В ходе этого этапа на основе анализа документов, представленных самим кандидатом, а также данных, полученных через Службу безопасности (документы об образовании и квалификации, социокарта, самопрезентация, заявление о приеме на работу, листки по учету кадров, рекомендательные письма, сведения о месте проживания и пр.), и результатов предварительного собеседования появляется определенная возможность отсечь те кандидатуры, которые по формальным признакам явно не соответствуют требованиям, предъявляемым к будущим сотрудникам.

2.3.3 Третий этап: тестовые процедуры и иные методики проверки кандидатов

Эта ступень характеризуется, как правило, комплексными психологическим тестированием. В последнее время значительную популярность приобретают многочисленные методы и процедуры персонального очного тестирования, поскольку они характеризуются быстротой реализации и достаточно высокой эффективностью. Каждый из этих методов имеет, конечно, свои ограничения, нарушение которых способны серьезно исказить полученные результаты.

Обычно тестовые методики подразделяются на четыре большие группы (Рисунок 2.1).

Личностные опросные листы. 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. На основе полученных данных формируются психологические характеристики испытуемых претендентов.

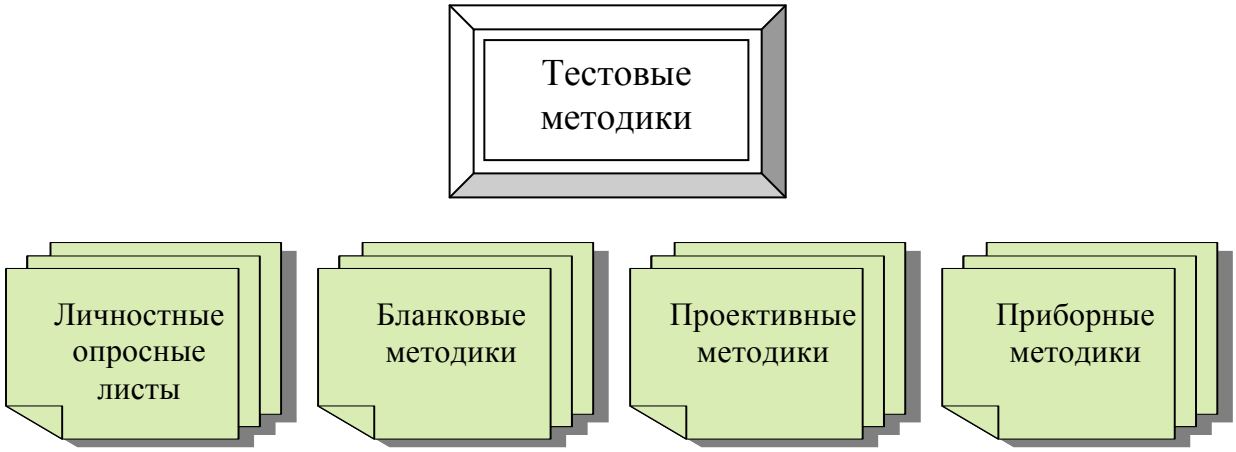

Рисунок 2.1 – Тестовые методики

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

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, Амтхауэра, методика компасов, таблицы Шульца и другие. Некоторые из них достаточно сложны и трудоемки в обработке и интерпретации результатов, вследствие чего имеют ограниченное применение в практике профессионального отбора.

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

Проективные методики. Эти процедуры представляют 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 Роршаха, 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 подобные методики используются пока еще редко, поскольку для их реализации требуются специальные помещения и наличие 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 конфиденциальной информации, касающейся кадровых проблем.

2.3.4 Методика проверки готовности персонала к действиям в чрезвычайных ситуациях

Необходимо отметить, что в условиях резкого обострения криминогенной обстановки некоторые предприятия уже вводят специальные тесты, направленные на выявление способностей кандидата активно и продуктивно действовать в сложных, кризисных условиях и чрезвычайных обстоятельствах, например, при возникновении очагов пожара, угрозах нападения под воздействием риска диверсионно-террористических проявлений (вероятность обстрелов, захватов, похищений, насилия и т.п.).

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

Таким образом, с одной стороны, тестирование дает 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 в процессе их обработки и интерпретации.

Итак, целью психологического тестирования является получение комплекса психологических характеристик на кандидата, которые в дальнейшем будут применяться для оценки его профессиональной пригодности. Кроме того, тестирование позволяет оценивать наличие и степень сформированности таких основополагающих черт характера как честность, искренность, лояльность, готовность к подчинению внутренним правилам.

Помимо этого опытные специалисты, использующие тестовые методики, стремятся выявлять следующие негативные черты характера кандидата: возбудимость, раздражительность, мнительность, беспокойство, повышенная чувствительность к замечаниям и рекомендациям, завышенная самооценка, необоснованное высокомерие и т.п.

2.3.5 Четвертый этап: заключительное собеседование

Итоговое собеседование является основным содержанием заключительной фазы работы с кандидатом. Как показывает опыт, именно на данном этапе, как это ни удивительно, сотрудники кадровых аппаратов и допускают наибольшее количество ошибок. Их главная причина кроется в том, что к самому факту собеседования относятся, как правило, формально. Имеется в виду то особое обстоятельство, что к данному моменту решение либо уже в целом принято, либо сформировано примерно на 90–95%. Именно поэтому заключительная беседа с

кандидатом сводится зачастую к уточнению лишь некоторых второстепенных вопросов и порой к окончательному согласованию отдельных пунктов трудового договора (контракта).

Перед началом заключительного собеседования рекомендуется составить примерный план беседы, обычно включающий следующие основные пункты:

1. Выделение основных вопросов, требующих обязательного дополнительного уточнения и разъяснения, итоги которых способны повлиять на окончательное решение о приеме кандидата на работу;

2. Определение узловых, принципиальных моментов в структуре и динамике беседы, в том числе последовательность и степень откровенности задаваемых вопросов, характер и продолжительность их обсуждения, различные варианты завершения собеседования;

3. Прогнозирование и моделирование вероятного поведения сотрудников кадрового аппарата, руководства, если в ходе собеседования вскроются новые и неожиданные обстоятельства, ставящие под сомнение возможность зачисления кандидата на работу;

4. Выбор оптимального времени, продолжительности, места проведения собеседования, которые должны быть удобными и приемлемыми для обеих сторон;

5. Формулирование психологических подходов к проведению заключительной фазы собеседования, которая, как правило, носит официальный характер, но должна располагать одновременно к свободному общению и определенному уровню доверительности.

2.4 Задачи службы безопасности при проведении проверки и отбора кандидатов на работу

С точки зрения обеспечения стратегических интересов предприятия обязательными являются следующие функции службы безопасности:

1. Определение степени вероятности формирования у кандидата преступных наклонностей в случаях возникновения в его окружении определенных благоприятных обстоятельств (персональное распоряжение кредитно-финансовыми ресурсами, возможность контроля за движением наличных средств и ценных бумаг, доступ к материально-техническим ценностям, работа с конфиденциальной информацией и пр.);

2. Выявление имевших место ранее преступных наклонностей, судимостей, связей с криминальной средой (преступное прошлое, наличие конкретных судимостей, случаи афер, махинаций, мошенничества, хищений на предыдущем месте работы кандидата и установление либо обоснованное суждение о его возможной причастности к этим преступным деяниям).

Для сбора сведений в рамках Закона о частной детективной и охранной деятельности в Российской Федерации следующие методы: опрос, анкетирование, целевые беседы с лицами по месту жительства кандидатов и на предыдущих местах их учебы или работы, наведение справок через медицинские учреждения и пр.

Необходимо быть абсолютно уверенным в том, что проводят тесты, собеседования и встречи именно с теми лицами, которые выступают в качестве кандидатов на работу. Это подразумевает идентификацию личности, тщательную

проверку паспортных данных, иных документов, а также получение фотографий кандидатов без очков, контактных линз, парика, макияжа. Необходимо требовать предоставления комплекта фотографий нескольких размеров (6х12, 4х6). Нужно быть готовыми и к попыткам спланированного проникновения представителей конкурентных или криминальных структур на ключевые посты структурных подразделений. По опыту работы силовых министерств Службы безопасности предприятий все чаще занимаются проверкой подлинности документов (паспорта, военного билета, дипломов, свидетельства о рождении и т.д.);

В связи с этим, рекомендуется настаивать на получении набора цветных фотографий кандидата, которые могут быть использованы в случае необходимости для предъявления жильцам по месту его проживания или коллегам по работе. Использование в кадровой работе цветных фотографий, соответствующих паспортным данным, предпочтительнее также в связи с тем, что они четко и без искажений передают цвет волос, глаз, кожи, возраст и характерные приметы кандидата.

В последние годы в динамично развивающихся организациях широко практикуется почерковедческая экспертиза, которая позволяет определять многие черты характера кандидата: темперамент, выдержку, волевые качества, собранность, аккуратность, грамотность, общеобразовательный уровень и пр., а также предрасположенность к совершению неблаговидных и нечестных поступков.

В том случае, если результаты указанных проверок, тестов и психологического изучения не противоречат друг другу и не содержат данных, которые бы препятствовали приему на работу данного кандидата, с ним заключается трудовое соглашение, в большинстве случаев предусматривающее определенный испытательный срок (1- 3 месяца).

2.5 Процедура увольнения кадров

Серьезное влияние на вопросы безопасности ведущих предприятий оказывают процедуры увольнения сотрудников.

Современные психологические подходы к процессу увольнения позволяют выработать следующую принципиальную рекомендацию: каковы 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, а чаще всего мнимых недостатках, промахах, ошибках в деятельности его прежних руководителей.

Таким образом, необходимо быть четко ориентированным 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.

2.5.1 Подготовка к беседе с увольняемыми сотрудниками

При поступлении устного или письменного заявления об увольнении в настоящее время широко практикуется во всех без исключениях случаях проведение с сотрудником беседы с участием психолога, представителя кадрового подразделения и обязательно кого-либо из руководителей предприятия. Однако 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 том числе конфиденциальной или составляющей коммерческую тайну;
- вероятный период устаревания конфиденциальных сведений, составляющих коммерческую тайну для данного предприятия;
- предполагаемое в будущем место работы увольняющегося (увольняемого) сотрудника.

Беседа при увольнении проводится только после того, когда собраны все необходимые сведения. Конечно, предварительно руководитель предприятия или лицо им уполномоченное отрабатывает принципиальный подход к вопросу о том, целесообразно ли предпринимать попытки склонить сотрудника изменить его первоначальное решение или же 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.

2.5.2 Проблема защиты коммерческой тайны при увольнении

Если 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 подписи о неразглашении данных, составляющих коммерческую тайну).

В этой связи необходимо подчеркнуть, что личное 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 самого предприятия. В этих обстоятельствах не следует поспешно реализовывать принятое решение. Если увольняемое лицо располагает какими-либо сведениями, составляющими коммерческую тайну, то целесообразно предварительно и под соответствующим предлогом перевести его на другой участок работы, например в такое подразделение, в котором отсутствует подобная информация.

Кроме того, таких лиц традиционно стремятся сохранить в структуре предприятия или его филиалов 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 после реализации этих мер рекомендуется приглашать на собеседование подлежащего увольнению сотрудника и объявлять конкретные причины, по которым предприятие отказывается от его услуг. Желательно при этом, чтобы выдвигаемые причины содержали элементы объективности, достоверности и очевидности, то есть, например, перепрофилирование производства, сокращение персонала, ухудшение финансового положения, отсутствие заказчиков и пр. При мотивации увольнения безусловно целесообразно воздерживаться от ссылок на негативные деловые и личных качества данного сотрудника.

Следует иметь ввиду, что даже намек на психологические причины может быть использован в суде для восстановления на работе или в печати для подрыва авторитета предприятия и его руководства.

2.5.3 Сохранение психологического контакта с увольняемыми сотрудниками

После объявления об увольнении рекомендуется дать увольняемому выговориться полностью. Следует внимательно выслушать контрдоводы, аргументы и замечания сотрудника в отношении характера работы, стиля руководства и т. п. Обычно увольняемый персонал весьма критично, остро и правдиво освещает ситуацию на предприятии, вскрывая уязвимые места, серьезные недоработки, кадровые просчеты, финансовые неурядицы и т. п. На некоторых предприятиях эту информацию даже записывают на магнитофон.

Если подходить не предвзято и объективно к подобной критике, то эти соображения могут быть использованы в дальнейшем весьма эффективно в интересах предприятия. В ряде случаев увольняемому сотруднику вполне серьезно 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 последующего трудоустройства на новом месте работы. При окончательном расчете обычно рекомендуется независимо от личностных характеристик увольняемых сотрудников брать у них подписку о неразглашении конфиденциальных сведений, ставших известными в процессе работ. Разглашение сведений возможно и вполне лояльными сотрудниками, так как они могут не

придавать этому серьезного значения, а их об этом при увольнении просто забыли предупредить.

В любом случае после увольнения сотрудников, осведомленных о серьезных сведениях, составляющих коммерческую тайну, целесообразно через возможности Службы безопасности или частного детективного агентства проводить оперативную проверку по их новому месту работы и моделировать возможные пути утечки конфиденциальных данных.

Кроме того, в наиболее острых и конфликтных ситуациях увольнения персонала должны проводиться оперативные и профилактические мероприятия по новому месту работы, жительства, также в окружении носителей коммерческих секретов.

2.5.4 Практические рекомендации

К категориям работников, имеющим доступ к коммерческой (в том числе конфиденциальной) информации, и которые могут быть потенциальными источниками ее разглашения, либо иных неправомерных действий, относятся прежде всего, работники бухгалтерии, кассиры, лица, имеющие право распоряжения печатями, бланками, работники компьютерных подразделений.

В практике работы с персоналом работники службы безопасности должны проверять не только хранение сотрудниками коммерческой тайны, но и отношение их своим служебным обязанностям, аккуратность в обращении с документами, излишний “интерес” к другим подразделениям.

Для работников службы безопасности индикаторами в выявлении конкретных работников, осуществляющих разглашение конфиденциальной информации, занимающихся хищением денег, либо совершающих другие неправомерные действия, угрожающие экономическому положению фирмы, являются следующие:

- внезапный активный интерес к конфиденциальной информации, деятельности других подразделений;
- изменение поведения работника в общении с коллегами, в разговорах, появление неуверенности, страха;
- резкое увеличение расходов работника, приобретение дорогостоящих товаров, недвижимости и пр.;

Потенциальными правонарушителями являются сотрудники:

- имеющие значительные материальные затруднения;
- имеющие склонность к азартным играм;
- склонные к пьянству, наркотической зависимости;
- имеющие тяжело больных близких родственников;
- часто меняющие место работы;
- психически неуравновешенные.

Для поддержания высокого уровня защищенности экономических интересов фирмы службе безопасности целесообразно проводить проверки лиц, которые могут, пользуясь своим служебным положением, представлять угрозы безопасности. Приведем некоторые способы таких проверок.

1. Лицу, ответственному за получение в банке денежных сумм, умышленного вкладывается в пачку лишняя купюра. Если лицо не реагирует на данные действия, то из этого могут быть сделаны следующие выводы:

- данное лицо небрежно относится к своим обязанностям;
- данное лицо умышленно присваивает деньги.

В обоих случаях есть основания сомневаться в личных, либо деловых качествах проверяемого лица.

2. Проверка выполнения исполнительно-распорядительных функций ответственным лицом. Работнику, имеющему право распоряжаться печатями, штампами. Посторонним лицом ему предлагается за вознаграждение проштамповать чистые листы бумаги. В случае согласия – доверие к такому лицу утрачивается и оно освобождается от должности.

3. Для банков. Проверяется лицо, обслуживающее клиентов в банке, имеющее право доступа к информации по счету и выдающее справки о наличии денежных средств на счетах клиентов. Один из клиентов (по просьбе работников службы безопасности) предлагает выдать ему справку о наличии значительной суммы денег у него на счете, хотя на самом деле эта сумма небольшая, обещая при этом приличное вознаграждение. Как правило, в выписке по счету к сумме дописывается один или два нуля. Понятно, что фиктивная справка необходима клиенту для введения в заблуждение контрагентов. В случае согласия работника банка можно сделать вывод о его неправомерном поведении.

Вообще же руководству предпринимательской фирмы необходимо проводить такую внутреннюю политику, чтобы минимизировать количество недовольных работников (служебным положением, оплатой труда и пр.) и особенно стараться сохранять хорошие отношения с увольняющимися работниками. В этом случае вероятность утечки информации будет снижена.

Вопросы для повторения темы:

1. На какие основные фазы можно разделить современный процесс отбора кадров?
2. Назовите основные группы, на которые подразделяются тестовые методики, используемые при отборе кадров?
3. При каком условии целесообразно использовать бланковые методики?
4. Что является целью психологического тестирования?
5. Раскройте принципиальное различие подходов по сохранению коммерческой тайны при увольнении сотрудника по решению руководства и по собственному желанию.
6. Влияет ли темперамент работника на процедуру заключительной беседы?
7. По каким признакам сотрудники службы безопасности могут отнести работника к потенциальным правонарушителям?

Литература:

1. Веснин В.Р. Технология работы с персоналом и деловыми партнерами. – М.: «Элит-2000», 2002.- 592с.
2. Грунин О., Грунин С. Экономическая безопасность в организации. – «Питер», 2002.- 160с.
3. Мэйган М. Работа с персоналом. Введение в должность. - «Питер», 2002. – 160с.
4. Степанов Л.Я. Управление персоналом: персонал в системе защиты

информации. – М.: «Инфра-М», 2002.- 288с.
5. Тверсов И.В. Правила работы с персоналом. – М.: «Даен», 2003.- 318с.
6. Шейнов В.П. Скрытое управление человеком. - М.: АСТ. -Минск: Харвест, 2002.- 848с.

Глава 3. Экономическая безопасность в информационной сфере

Ключевые понятия:

Конфиденциальная информация
Коммерческая тайна
Бланк строгой отчетности
Телефонные радиомикрофоны
Акустические радиомикрофоны
Комбинированные радиомикрофоны
Высшая степень конфиденциальности
Информация ограниченного доступа
Лазерные микрофоны
электронные стетоскопы
сканирующих приемниках
Направленные микрофоны
Бланк
Держатель
Источник
Злоумышленник
Шумогенераторы
Шифраторы
Маскираторы
Утечка информации
Разглашение
Несанкционированный доступ
Открытая информация
Банковская тайна

3.1 Общие положения

В процессе определения ценности информации необходимо учитывать следующие факторы: свойства самой информации, возможные виды угроз и действия злоумышленника (вероятные способы получения информации).

Ценность информации можно условно классифицировать по четырем категориям важности (Таблица 3.1).

В реальных условиях определение важности информации предприятия может представлять собой очень трудную задачу, так как одна и та же информация может быть использована различными подразделениями предприятия как государственных, так и частных, каждое из которых может отнести эту информацию к различным категориям важности. Кроме того, категория важности определенной информации со временем изменяется, например из-за ее старения.

Таблица 3.1 – Классификация информации по важности

Жизненно важная	-незаменимая информация, наличие которой необходимо для нормального функционирования объекта защиты (предприятия).
Важная	-информация, которая может быть заменена или восстановлена, но процесс восстановления очень труден и связан с большими затратами.
Полезная	-информация, которая полезна и которую трудно восстановить, однако предприятие может эффективно функционировать и без нее.
Несущественная	-информация, которая больше не нужна предприятию.

Рассмотрим три группы лиц, имеющих или стремящихся получить доступ к информации, обрабатываемой в автоматизированной информационной системе предприятия.

Держатель (владелец) - организация или отдельное лицо (например, пользователь системы), которое обладает ценной информацией и использует ее для своих целей.

Источник - организация или отдельное лицо (например, заказчик), которое поставляет информацию или к которому относится информация.

Злоумышленник - отдельное лицо или Организация (например, конкурирующая организация), которая стремится получить ценную информацию, но в нормальных условиях не имеет доступа к ней.

Вся эта информация представляет различную ценность для самого предпринимателя и, соответственно, ее разглашение может привести (либо не привести) к угрозам экономической безопасности различной степени тяжести. Поэтому информацию необходимо разделить на три группы:

- информация для открытого пользования любым потребителем в любой форме;
- информация ограниченного доступа – только для органов, имеющих соответствующие законодательно установленные права (милиция, налоговая полиция, прокуратура);
- информация только для работников (либо руководителей) фирмы.

Информация относящаяся ко второй и третьей группам является конфиденциальной и имеет ограничения в распространении.

Конфиденциальная информация – это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ. Часть этой коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Коммерческая тайна, в соответствии с гражданским законодательством РФ, это информация которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель принимает меры к охране ее конфиденциальности. Следовательно, коммерческая тайна не может быть общеизвестной и общедоступной информацией, открытое ее использование несет угрозу экономической безопасности предпринимательской деятельности, в связи с чем предприниматель осуществляет меры по сохранению ее конфиденциальности и защите от незаконного использования.

Однако не вся информация, которой располагает предприниматель, может быть отнесена к категории коммерческой тайны. Существует официально утвержденный перечень сведений, которые не могут составлять коммерческую тайну в РФ. К ним относятся:

- информация, составляющая государственную тайну;
- информация, содержащаяся в учредительных документах, дающих право заниматься предпринимательской деятельностью (регистрационных удостоверениях, лицензиях и других);
- информация, содержащаяся в годовых отчетах, бухгалтерских балансах,

формах годовой бухгалтерской отчетности, в том числе в аудиторских заключениях, а также в иных документах, связанных с исчислением и уплатой налогов и других обязательных платежей;

- информация, содержащая сведения об оплачиваемой деятельности государственных служащих, о задолженностях работодателей по выплате заработной платы и другим выплатам социального характера, о численности и составе работников, о наличии свободных рабочих мест;
- информация об использовании имущества, содержащаяся в годовых отчетах фондов;
- информация, подлежащая раскрытию эмитентом ценных бумаг, профессиональным участником рынка ценных бумаг и владельцем ценных бумаг в соответствии с законодательством Российской Федерации о ценных бумагах;
- информация о деятельности благотворительных организаций и иных некоммерческих организаций;
- информация о хранении, об использовании или перемещении материалов и об использовании технологий, представляющих опасность для жизни и здоровья населения или окружающей среды, о соблюдении экологического и антимонопольного законодательства, об обеспечении безопасных условий труда, о реализации причиняющей вред здоровью населения продукции, о других нарушениях законодательства Российской Федерации, а также информация, содержащая сведения о размерах причиненных при этом убытков;
- информация о реализации государственных программ приватизации и об условиях приватизации конкретных объектов;
- информация о размерах имущества и вложенных средствах при его приватизации;
- информация о ликвидации юридического лица, порядке и сроках заявлений требований его кредиторами;
- информация, для которой введены ограничения на установление режима коммерческой тайны федеральным законом или принятым в соответствии с ним иным нормативным актом.

Как в РФ так и во всем мире увеличивается число информационных преступлений, что может привести, в конечном счете, к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать.

Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание безопасности и работоспособности информационных систем.

3.2 Виды угроз информационным объектам

Общая классификация угроз автоматизированной информационной системе объекта представлены в таблице 3.2.

Оценка уязвимости автоматизированной информационной системы и построение модели воздействий предполагают изучение всех вариантов реализации перечисленных выше угроз и выявления последствий, к которым они приводят.

Таблица 3.2 - Общая классификация угроз автоматизированной информационной системы

Угрозы конфиденциальности данных	Реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи. Информация, обрабатываемая на компьютерах или передаваемая по локальным сетям передачи данных, может быть снята через технические каналы утечки. При этом используется аппаратура, осуществляющая анализ электромагнитных излучений, возникающих при работе компьютера. Такой съем информации представляет собой сложную техническую задачу и требует привлечения квалифицированных специалистов. С помощью приемного устройства, выполненного на базе стандартного телевизора, можно перехватывать информацию, выводимую на экраны дисплеев компьютеров с расстояния в тысячу и более метров. Определенные сведения о работе компьютерной системы извлекаются даже в том случае, когда ведется наблюдение за процессом обмена сообщениями (трафиком) без доступа к их содержанию.
Угрозы целостности данных	Целостность данных нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой. Несанкционированная модификация информации о безопасности системы может привести к несанкционированным действиям (неверной маршрутизации или утрате передаваемых данных) или искажению смысла передаваемых сообщений.
Угрозы доступности данных	Возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. Эта угроза реализуется захватом всех ресурсов, блокированием линий связи несанкционированным объектом в результате передачи по ним своей информации или исключением необходимой системной информации. Эта угроза может привести к ненадежности или плохому качеству обслуживания в системе и, следовательно, потенциально будет влиять на достоверность и своевременность доставки платежных документов.
Угрозы отказа от выполнения трансакций	Возникают в том случае, когда легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность.

Угрозы могут автоматизированной информационной системе объекта быть обусловлены следующими факторами (Рисунок 3.1):

1. Естественные факторы (стихийные бедствия пожар, наводнение, ураган, молния и другие причины);

2. Человеческие факторы подразделяются на:

а) пассивные угрозы (угрозы, вызванные деятельностью, носящей случайный, неумышленный характер). Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны для воссоединения с семьей и т.п.);

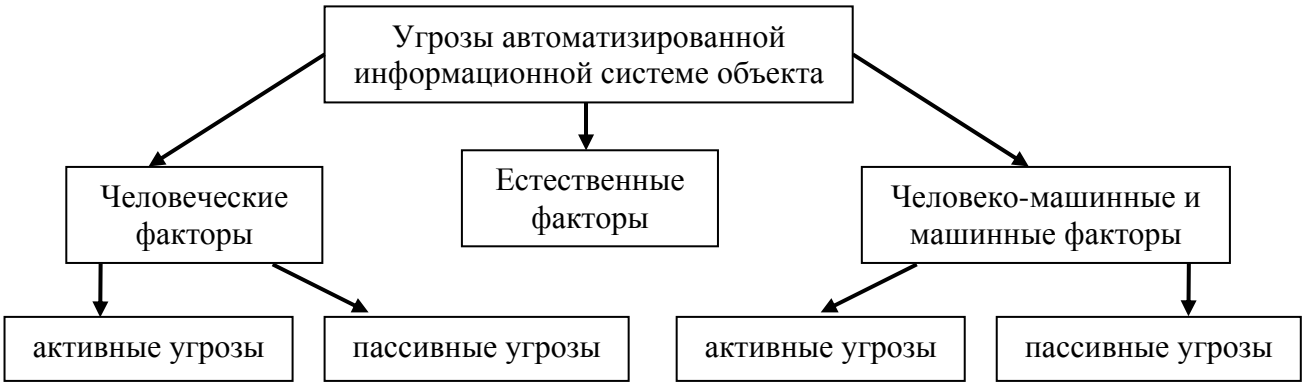

Рисунок 3.1 - Угрозы автоматизированной информационной системе объекта

б) активные угрозы (угрозы, обусловленные умышленными, преднамеренными действиями людей). Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений, секретов производства, новых технологий по корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); просмотром и передачей различной документации, просмотром «мусора»; подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний, информации (например, в связи с получением другого гражданства по корыстным мотивам);

3. Человеко-машинные и машинные факторы, подразделяются на:

а) пассивные угрозы. Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.); с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

б) активные угрозы. Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной технику и каналам связи, хищение различных видов носителей информации: дискет, описаний, распечаток и других материалов, просмотр вводимых данных, распечаток, просмотр «мусора»); угрозы, реализуемые бесконтактным способом (сбор электромагнитных излучений, перехват сигналов, наводимых в цепях (токопроводящие коммуникации), визуально-оптические способы добычи информации, подслушивание служебных и научно-технических разговоров и т.п.).

Основными типовыми путями утечки информации и несанкционированного доступа к автоматизированным информационным системам, в том числе через каналы телекоммуникаций, являются следующие:

1) перехват электронных излучений;

2) принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;

3) применение подслушивающих устройств (закладок);
4) дистанционное фотографирование;
5) перехват акустических излучений и восстановление текста принтера;
6) хищение носителей информации и производственных отходов;
7) считывание данных в массивах других пользователей;
8) чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
9) копирование носителей информации с преодолением мер защиты;
10) маскировка под зарегистрированного пользователя;
11) мистификация (маскировка под запросы системы);
12) незаконное подключение к аппаратуре и линиям связи;
13) использование «программных ловушек».

Возможными каналами преднамеренного несанкционированного доступа к информации при отсутствии защиты в автоматизированной информационной системе могут быть:

- штатные каналы доступа к информации (терминалы пользователей, средства отображения и документирования информации, носители информации, средства загрузки программного обеспечения, внешние каналы связи) при их незаконном использовании;
- технологические пульты и органы управления;
- внутренний монтаж аппаратуры;
- линии связи между аппаратными средствами;
- побочное электромагнитное излучение, несущее информацию;
- побочные наводки на цепях электропитания, заземления аппаратуры, вспомогательных и посторонних коммуникациях, размещенных вблизи компьютерной системы.

Способы воздействия угроз на объекты информационной безопасности представлены в таблице 3.3.

3.3 Работа с конфиденциальными документами

Конфиденциальная информация, в том числе коммерческая тайна, как правило, содержится в виде каких-либо документов – традиционных, бумажных, либо электронных. Эти источники информации могут являться объектами неправомерных посягательств и, следовательно, нуждаются в защите. Конфиденциальная информация на крупных предприятиях, предприятиях имеющих нескольких собственников представляет собой более сложный объект защиты.

Все документы в фирме делятся на три категории: входящие, исходяшие и внутренние. Первым шагом в обеспечении защиты информации является выявление из общей массы документов, содержащих ценную для фирмы коммерческую информацию. Составляется перечень конфиденциальных документов. Затем вводятся степени конфиденциальности информации (или грифы ограничения доступа к документам) и каждому документу присваивается соответствующий гриф. Данный перечень составляется специальной комиссией (в крупных фирмах), либо секретарем-референтом фирмы (специальным сотрудником). Потом он согласовывается с начальниками отделов, служб и утверждается руководителем фирмы.

Таблица 3.3 – Детализация способов воздействия угроз на объекты информационной безопасности

Информационные способы	⁎ нарушение адресности и своевременности информационного обмена, противозаконный сбор и использование информации; ⁎ несанкционированный доступ к информационным ресурсам; ⁎ манипулирование информацией (дезинформация, сокрытие или искажение информации); ⁎ незаконное копирование данных в информационных системах; ⁎ нарушение технологии обработки информации.
Программно-математические способы	⁎ внедрение компьютерных вирусов; ⁎ установку программных и аппаратных закладных устройств; ⁎ уничтожение или модификацию данных в автоматизированных информационных системах.
Физические способы	⁎ уничтожение или разрушение средств обработки информации и связи; ⁎ уничтожение, разрушение или хищение машинных иди других оригинальных носителей информации; ⁎ хищение программных или аппаратных ключей и средств криптографической защиты информации; ⁎ воздействие на персонал; ⁎ поставка «зараженных» компонентов автоматизированных информационных систем.
Радиоэлектронные способы	⁎ перехват информации в технических каналах ее возможной утечки; ⁎ внедрение электронных устройств перехвата информации в технические средства и помещения; ⁎ перехват, дешифровка и навязывание ложной информации в сетях передачи данных и линиях связи; ⁎ радиоэлектронное подавление линий связи и систем управления.
Организационно-правовые способы	⁎ невыполнение требований законодательства и задержки в принятии необходимых нормативно-правовых положений в информационной сфере; ⁎ неправомерное ограничение доступа к документам, содержащим важную для граждан и организаций информацию.

В перечне документов указываются категории работников, которые по должности могут пользоваться этими документами. Гриф ограничения доступа к документу устанавливается на определенный срок. Каждый документ, отнесенный к той или иной степени конфиденциальности должен на титульном (первом) листе иметь в правом верхнем углу пометку о грифе.

Порядок работы с документами, составляющими коммерческую тайну, регламентируется специальной инструкцией по закрытому делопроизводству, которая регулирует порядок документирования и организации работы с конфиденциальными документами, включающей следующие разделы:

“**Общие положения**” - на основе действующего законодательства и нормативно-методических документов определяется понятие коммерческой тайны, устанавливаются цели данной инструкции, определяются люди или подразделения, ответственные за работу с документами, составляющими коммерческую тайну;

“**Документирование деятельности фирмы, составляющей коммерческую тайну**” - определяются виды конфиденциальных документов, порядок их

подготовки и оформления, присваиваемые грифы ограничения доступа к документам;

“**Организация работы с документами**” – устанавливается порядок присвоения грифов и правила работы с документами, содержащими коммерческую тайну.

Процесс обеспечения сохранности информации в документах содержащих коммерческую тайну осуществляется в соответствии с основными стадиями “жизненного” цикла документа. Этими стадиями являются:

1. **Получение (отправка) документа**. Документ, поступающий в фирму и содержащий гриф конфиденциальной информации, должен быть передан только секретарю-референту или инспектору закрытого делопроизводства и зарегистрирован. Далее, он передается руководителю, а последний определяет непосредственного исполнителя по данному документу, имеющему допуск к этой категории документов, и адресует документ ему. Аналогичный порядок при отправлении документа – подготовка документа, подпись руководителя, регистрация в специальном журнале секретарем-референтом и отправка.
2. **Хранение документа**. Все документы, содержащие конфиденциальную информацию, должны храниться в специально отведенных, закрывающихся помещениях, в запертых шкафах, столах или ящиках. Документы же составляющие коммерческую тайну – только в металлических сейфах, оборудованных сигнализацией. Все помещения должны опечатываться. Следует иметь в виду, что при определении степени конфиденциальности документа производится также определение срока в течение которого она действует. По истечении срока возможны различные действия:
   1) гриф может быть продлен,
   2) гриф может быть снят и документ становится открытым,
   3) документ уничтожается.
3. **Использование документа**. Система доступа сотрудников, не имеющих соответствующих прав по должности, к конфиденциальным документам должна иметь разрешительный характер. Каждая выдача таких документов регистрируется (расписываются оба сотрудника – и тот, кто берет документ, и тот, кто его выдает) и проверяется порядок работы с ними (например, нарушением считается оставление данных документов на столе во время обеда, передача другим лицам, вынос за пределы служебных помещений).
4. **Уничтожение документа**. Конфиденциальные документы, утратившие практическое значение и не имеющие какой-либо правовой, исторической или научной ценности, срок хранения которых истек (либо не истек), подлежат уничтожению. Для этого создается комиссия (не менее 3 человек) в присутствии которой производится уничтожение. Затем члены комиссии подписывают акт об уничтожении. Бумажные документы уничтожаются путем сожжения, дробления, превращения в бесформенную массу, а магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и др.
5. **Контроль** за соблюдением правил хранения и использования документов, содержащих конфиденциальную информацию, осуществляется с помощью проверок. Они могут быть как регулярными (еженедельными, ежемесячными, ежегодными), так нерегулярными (выборочными, случайными). В случае

обнаружения нарушений составляется акт и принимаются меры, позволяющие в будущем предотвратить нарушения такого рода.

Следует контролировать не только документы, содержащие конфиденциальную информацию, но и бумаги с печатями, штампами, бланки.

Бланк – лист бумаги с оттиском углового или центрального штампа, либо с напечатанным любым способом текстом (или рисунком), используемый для составления документа.

Особое внимание следует уделять охране так называемых бланков строгой отчетности.

Бланк строгой отчетности – бланк, содержащий номер (серию), зарегистрированный одним из установленных способов и имеющий специальный режим использования.

Важным направлением в организации работы по защите конфиденциальной информации является установление порядка обращения с ее носителями. При этом следует учитывать, что:

- специалисты ставят обязательным условием наличие на носителях конфиденциальной информации отличительных пометок, различающихся в зависимости от уровня секретности, но они должны отличаться от применяемых в сфере защиты государственных секретов;
- в условиях фирмы обеспечить каждому исполнителю работу в специально выделенном помещении бывает практически невозможно, поэтому следует соблюдать "политику чистых столов". Суть ее заключается в том, что в отсутствие работника на его рабочем месте не должно быть никаких документов.

Существует миф о том, что в зарубежных фирмах на каждом шагу стоят ксероксы и сделать копию с любого документа не составляет труда любому желающему. Это абсолютно не соответствует действительности: в любой фирме, имеющей дело с конфиденциальной информацией, существует строго установленный порядок размножения документов. С целью затруднить или даже сделать невозможным копирование закрытых материалов принимаются дополнительные меры защиты. Так, американская фирма "Ксерокс" разработала специальный краситель, который наносится на текст документа, что исключает возможность несанкционированного копирования - копия получается нечитабельной.

Руководитель должен упорядочить процессы фиксации секретной информации в деловых бумагах и организовать их движение таким образом, чтобы похищение конфиденциальных документов было бы затруднено настолько, чтобы оно становилось экономически невыгодным для похитителя.

При работе с документами, содержащими коммерческую тайну, следует соблюдать определенные правила, которые сводятся к нижеследующим:

1) строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;

2) назначение ответственных лиц за контролем секретного делопроизводства и наделение их соответствующими полномочиями;

3) разработка инструкции (памятки) по работе с секретными документами, ознакомление с ней сотрудников фирмы;

4) контроль за принятием служащими письменных обязательств о

сохранении коммерческой тайны фирмы;

5) введение системы материального и морального поощрения сотрудников, имеющих доступ к секретной информации;

6) внедрение в повседневную практику современных технологий защиты коммерческой тайны фирмы;

7) личный контроль со стороны руководителя фирмы за службами внутренней безопасности и секретного делопроизводства.

Существуют различные способы ведения секретного делопроизводства, которые направлены на предотвращение утечки содержащихся в документах коммерческих секретов. Как уже было указано выше, документы, содержащие коммерческую тайну, подразделяются по степени секретности имеющейся в них информации и снабжаются соответствующей пометкой.

Грамотно поставленная работа с документами поможет защитить их от постороннего глаза. Не следует держать на столе сразу несколько документов, да к тому же различных по степени значимости.

При работе с документами не отлучайтесь из комнаты, а если приходится выходить, то не забудьте закрыть дверь.

Посторонних к документам допускать не следует. Документы, которые правомерно могут потребовать сотрудники налоговой инспекции или правоохранительных служб, следует держать отдельно от остальных конфиденциальных бумаг.

По окончании работы наиболее важные документы убираются в сейф, менее важные - в специальные контейнеры. Те и другие следует опечатать и сдать на хранение сотрудникам службы безопасности фирмы.

При пересылке документов следует иметь в виду, что использование телемониторов-игл позволяет через непроклеенные уголки конвертов прочитать содержимое делового письма, не вскрывая его. Поэтому конверты с документами целесообразно дополнительно проклеить скотчем.

Доверяя свои бумаги почте, отправляйте их заказными письмами с уведомлением о вручении их адресату.

Перемещение документов внутри фирмы также следует держать под контролем.

Организация защиты документов - обязанность руководителя фирмы и ее службы безопасности. Следует быть уверенным, что с момента появления и до уничтожения документ к посторонним не попадал. Если документ утерян (украден), специалисты по службе безопасности должны провести расследование.

Подготовку документов, содержащих важные сведения, следует доверять проверенным людям. Количество экземпляров должно быть строго ограниченным. Для разделения документов по степени важности можно использовать яркие цветные наклейки. При необходимости следует определять степень конфиденциальности документов, а также срок действия ограничительных грифов.

При этом следует помнить: чем больше секретной информации в нем отражено, тем больше потребуется затрат для его защиты.

Копирование документов - один из способов получения сведений, составляющих тайну фирмы. Множительная техника должна находиться под

надежным контролем. Количество копий должно строго учитываться, а их уничтожение - контролироваться. Придерживайтесь правила: наиболее ценные документы руководители фирм копируют сами.

Если документы размножаются на принтерах ЭВМ, то следует позаботиться о защите информации на магнитных носителях. Если это пишущая машинка нового поколения, то следует принять меры по хранению перфоленты, позволяющей повторно печатать один и тот же текст в автоматическом режиме. Да и по стуку клавишей пишущей машинки специалист с помощью электроники получит текст, аналогичный оригиналу, находясь вне помещения вашего офиса.

Для работы с секретными документами должны отводиться специальные помещения с хорошей звукоизоляцией. В эти помещения не должны допускаться не только посторонние лица, но и сотрудники, не имеющие разрешения (допуска) на работу с секретами фирмы. Эти помещения должны иметь капитальные стены, надежные перекрытия, прочные двери со спецзамками и запорами, защиту на окнах от проникновения посторонних лиц. Эти помещения должны надежно охраняться, в том числе системой охранной сигнализации, электронно-механическими приспособлениями, системами кабельного телевидения и т.п.

Черновики секретных документов должны готовиться в тетрадях с пронумерованными листами. После подготовки документов "набело" черновики должны уничтожаться уполномоченными на то сотрудниками. Число копий секретных документов должно строго учитываться, а копировальные машины снабжаться счетчиком копий и ключом, запускающим машины в действие.

Копировальная бумага и красящая лента пишущих машин - предмет особых забот, так как с них можно снять секретную информацию. Поэтому использованная копировальная бумага и лента уничтожаются под контролем ответственных лиц.

Вероятность утечки секретной информации из документов особенно велика в процессе их пересылки. Если нет возможности пользоваться услугами военизированной фельдсвязи, то доставку секретных документов и ценностей следует организовать своими силами с привлечением сотрудников собственной службы безопасности или же обратиться в специализированные фирмы, которые такие услуги оказывают за плату.

Служащие фирмы, отвечающие за сохранность, использование и своевременное уничтожение секретных документов, должны быть защищены от соблазна торговли секретами фирмы простым, но весьма надежным способом - хорошей зарплатой.

В процессе хранения и пересылки секретных документов могут быть применены средства защиты и сигнализации при несанкционированном доступе к ним. Одна из новинок - светочувствительное покрытие, наносимое на документы, которое может проявиться под воздействием света, указывая тем самым на факт ознакомления с документами или их фотографированием посторонними лицами.

Используют в этих целях и электронику. Устройство величиной со спичечный коробок реагирует на свет. Стоит его включить и поместить в сейфе или под бумагами на рабочем столе - и в вашем распоряжении надежный сторож. Электронное устройство срабатывает при попадании на него света и подает пронзительный звуковой сигнал. Это устройство называется "Home detective" (Домашний детектив). По желанию заказчика фирма снабжает "Home detective"

радиопередатчиком, включающим на значительном расстоянии иные защитные системы и внешнюю сигнализацию.

Специалистам по вопросам защиты коммерческой информации известны и иные технологии и системы охраны конфиденциальных документов от несанкционированного доступа или возможной утечки из них охраняемых сведений.

3.4 Техника съема информации

Сегодня электронные средства, предназначенные для промышленного шпионажа, доведены до высокого уровня совершенства. А самая распространенная техника для съема информации - радиомикрофоны. В народе их называют "жучками" или "клопами", специалисты именуют их "закладками". Они бывают:

- телефонными;
- акустическими;
- комбинированными;
- направленного действия;
- лазерными.

Телефонные радиомикрофоны снимают передаваемую по телефонной сети информацию и передают ее на специальный приемник или FM-радио на расстояние от 50 до 200 метров. Они устанавливаются в телефонные аппараты, розетки, а также вживляются в провода телефонных линий. "Телефонки" делятся на линейные и индукционные. Первые включаются в телефонную линию параллельно, одновременно снимая информацию и получая электропитание. Вторые же крепятся на один из проводов телефонной пары. Питание индукционных закладок осуществляется компактными батареями, что ограничивает время действия от шести часов до двух суток и сказывается на их размерах. Обнаружение таких радиомикрофонов крайне затруднено, так как их подключение не влияет на сопротивление линии.

Акустические радиомикрофоны ретранслируют все звуки, раздающиеся в помещении, на приемник оператора. Широко распространены акустические закладки, вмонтированные в шариковую ручку, пачку сигарет, зажигалку, электрический удлинитель, плинтус, тройник или настольную лампу.

Комбинированные радиомикрофоны совмещают в себе функции линейных и акустических. Монтируются они исключительно в телефонных аппаратах и розетках и ведут попеременный контроль как телефонных переговоров, когда трубка телефона снята, так и любых разговоров в помещении, когда трубка положена на рычаг. Питание осуществляется, как правило, за счет телефонной линии.

Направленные микрофоны отличаются от обычных узким сектором перехвата от 2 до 45 градусов и высокой чувствительностью. Это позволяет слышать разговор на расстоянии до 70 метров. Необходимо только направить микрофон в сторону говорящих. Единственное условие между оператором и объектом прослушивания не должно быть стен, заборов, зданий и транспортных коммуникаций с интенсивным движением, издающих постоянный шум. Направленные микрофоны обычно маскируются под трости, зонты, кейсы и снабжены либо наушниками, либо микропередатчиком, ретранслирующим информацию на специальный приемник.

Лазерные микрофоны используются для дистанционного контроля помещений и автомобилей. Их действие основано на анализе микроколебаний оконных стекол, возникающих от акустических колебаний внутри помещения. Лазерные микрофоны устанавливаются только на неподвижную поверхность и плохо работают вблизи оживленных магистралей. Несмотря на высокую цену и жесткие ограничения по применению, они пользуются спросом, ибо обнаружить это прослушивание практически очень трудно.

Существует и "оружие ближнего боя" - **электронные стетоскопы**. С их помощью прослушивают разговоры сквозь двери и стены толщиной до 70 сантиметров. Кстати, в 99% зданий толщина стен не превышает 70 сантиметров. Этот вид прослушивания, как и лазерный, определить достаточно сложно.

Особо следует упомянуть о средствах перехвата радиопереговоров - **сканирующих приемниках**. В Россию они в основном попадают из-за рубежа. С помощью сканеров осуществляют прослушивание разговоров, ведущихся по офисным радиотелефонам, аппаратам сотовой и спутниковой связи, а также радиостанциям. Такое прослушивание возможно только в том случае, когда оператор сканера находится в пределах радиуса действия контролируемого радиопередатчика.

На рисунке 3.2 показаны различные варианты "проникновения" в закрытое помещение с целью похищения секретной информации:

1. Лазерная система подслушивания разговоров по вибрации стекол
2. Магнитофон, принимающий сигналы от "жучка", вмонтированной в окно.
3. Телекамера, соединенная с оптическими волокнами в стене.
4. "Жучок" связанный с окном "напрямую".
5. Система считывания данных с экрана компьютера.
6. "Жучки" в телефонной сети.
7. Приемник сигналов от "жучка", реагирующего на стук клавише пишущей машинки.
8. Источник и приемник "пассивных" микроволн.
9. "Жучок" в выключателе освещения.
10. Микрофон узконаправленного действия.

3.5 Средства защиты информации

Индустрия прослушивания породила индустрию защиты от него. Расценки на обследование помещения на наличие "жучков" доходят до 5 долларов за квадратный метр.

На каждый вид подслушивающей аппаратуры имеется свое "противоядие". Иногда те же приборы, которые используются для съема информации. Так, сканеры применяются и для поиска скрытых радиомикрофонов.

А вот для того, чтобы найти и обезвредить "жучок", необходим индикатор поля. Чем ближе прибор придвигается к скрытому радиомикрофону, тем громче и чаще он издает звук, тем ярче разгорается лампочка, тем выше показатели на измерительной шкале. Круг поиска сужается, пока индикатор не начнет зашкаливать. Именно эта часть офиса тщательно обследуется.

Существуют анализаторы телефонных линий, применяющиеся до контроля за прослушиванием. Действие этих приборов основано на измерении электрического

Рисунок 3.2 - жучки

сопротивления линии и сопоставления его с нормальной величиной. Анализаторы успешно применяются против "телефонок" линейного типа, но они бессильны против индукционных "закладок".

Выявленные радиомикрофоны обнаруживаются путем осмотра всего доступного отрезка телефонной линии, а также телефонного аппарата. Иногда применяется такое средство ликвидации "закладок", как разрядник. Предварительно отключив от телефонной сети всю оргтехнику, разрядник соединяют с телефонной розеткой и включают. Электрический импульс высокого напряжения до нескольких тысяч вольт принимают на себя подслушивающие устройства. Конечно, страдает оборудование АТС, но связь сохраняется, а "закладка" прекращает свое существование.

Для сохранения конфиденциальности переговоров используются обнаруживатели диктофонов. Несмотря на высокую цену (до 1000 долларов США), такие приборы пользуются популярностью среди бизнесменов и политиков.

Существуют также средства превентивной защиты информации. К ним относятся шумогенераторы и шифраторы.

Шумогенераторы создают постоянные помехи (шумы), которые затрудняют или делают работу подслушивающих устройств невозможной. Наиболее часто шумогенераторы применяются для подавления радиомикрофонов различных типов. Но проблемы это не снимает: появились записывающие дискретные "жучки", которые выдают информацию длиной в секунду всего несколько минут в сутки в цифровом виде.

Несколько другой метод помех создают шумогенераторы для окон. Укрепленные на стеклах, они испускают микровибрации с постоянным изменением периодичности. Эти помехи делают невозможной работу лазерного микрофона.

Шифраторы обеспечивают кодирование телефонных и радиопереговоров. Различают три класса кодирования информации.

Маскираторы - наиболее распространенный и наименее устойчивый к декодированию класс приборов. Защита от прослушивания обеспечивается тем, что аппарат кодирования, подключенный к телефону, разбивает речь абонента на определенные отрезки и тасует их как колоду карт. Этот метод шифрации называется инверсией спектра, а аппараты, которых он использован, - инверторами. Чаще всего они имеют форму подставки под телефонный аппарат или накладки на телефонную трубку. Для радиостанций выпускаются специальные инверсионные платы, встраиваемые внутрь корпуса. Несмотря на кажущуюся надежность подобной системы защиты, время, требуемое на дешифровку подобной системы, исчисляется несколькими часами.

Надежнее аппаратура временной стойкости. Время, необходимое для подбора ключей, варьируется от нескольких дней до многих месяцев. И, наконец, системы постоянной стойкости обеспечивают своим пользователям гарантированное сохранение конфиденциальной информации. Принцип действия таких систем заключается в непрерывной смене не только ключей кодирования, но и самой системы смены ключей.

Защиту (шифровку) специалисты делят на мягкую и жесткую. К мягкой относят такую, которую можно взломать (расшифровать) за десять минут, к жесткой - над которой ломать голову придется несколько лет. Качественная защита обеспечивается качественной техникой. Получить разрешение на приобретение

такой аппаратуры можно только с разрешения ФАПСИ. Попытаться купить шифровальное устройство у умельца-одиночки тоже можно, но надеяться на то, что его не "взломают" специалисты, несерьезно.

Перед тем как остановить свой выбор на какой-то определенной системе защиты, подсчитайте, сколько вы потеряете в случае утечки информации. Сумма расходов на технику несанкционированного съема информации очень редко превышает 20% от ожидаемой прибыли. Помните, что излишняя экономия на безопасность часто выходит боком, но и перебарщивать не стоит. Так, например, от лазерного микрофона ваши окна могут защитить не только супер сложные генераторы помех. Плотные и тяжелые плюшевые шторы хорошо скрадывают микровибрацию. Очень хороши в этом отношении и многослойные стеклопакеты.

Вакуум между стеклами пакета не только защищает помещение от холода, но и препятствует прохождению микроколебаний, порождаемых голосом. Возможна и установка в окнах кривых звукоискажающих стекол или же можно вставить в раму толстое неровное стекло, которое меньше вибрирует, рассеивает отраженный луч хаотично и не может служить мембраной в случае наведения на него мощного источника электромагнитных излучений.

Принимая подарки и сувениры, Вы можете принести к себе или в офис "закладку". Согласно нормам этикета от подарков отказываться не следует, но на этот случай обзаведитесь индикатором поля и тщательно проверяйте каждую вещь, полученную Вами из чужих рук. Следует иметь в виду, что применение радиомикрофонов, лазерных направленных микрофонов, траверсов, электронных стетоскопов и минивидеокамер организациями и частными лицами, не имеющими на это специальных полномочий, категорически запрещено законом.

В соревновании "слухачей" и "защитников" первые сделали солидный отрыв с появлением СВЧ-излучения. Новый метод прослушивания позволяет снимать информацию с любого прибора в офисе, даже читает текст на мониторе компьютера. Блокировать СВЧ невозможно. Защита может быть только одна - расставить часовых в радиусе ста метров вокруг здания. С такого расстояния СВЧ не действует.

Рабочие помещения, служебные кабинеты должны быть закрыты для посещения посторонними лицами. Всех посетителей, кроме клиентов и деловых партнеров, должны встречать и сопровождать по территории фирмы работники отдела кадров, службы внутренней безопасности или охраны. Прием посетителей и работа с ними проходит в специально оборудованных техническими средствами охраны и сигнализации помещениях.

На многих предприятиях промышленно развитых стран посетителям выдаются разовые карточки (пропуска) гостя, размещаемые на груди или на лацкане пиджака. Карточки окрашены в яркие цвета. Доступ в те или иные помещения фирмы определяются цветом гостевой карточки. Передвижение гостя, таким образом, контролируется не только сопровождающими его лицами, но и остальным персоналом фирмы.

Некоторые помещения в любом случае должны оставаться недоступными для посещения всеми без исключения посторонними лицами, а также сотрудниками фирмы, не допущенными к работе с ее секретами. Эти помещения - святая святых. К ним относятся хранилища секретных документов, комнаты для работы с ними, зал совещаний, определенные подразделения фирмы, такие как: отдел маркетинга,

служба внутренней безопасности, аналитический отдел. Все эти помещения находятся в зоне безопасности, которая запретна для доступа посторонним лицам, строго охраняется и периодически проверяется на возможное наличие в ней технических средств промышленного шпионажа. Эта зона - объект особых забот для службы внутренней безопасности. Ее стерильность от электронных средств, предназначенных для промышленного шпионажа, во многом обеспечивает экономическую безопасность и конкурентоспособность фирмы, ее выживание в условиях рыночной экономики.

3.6 Защита секретной информации

Сегодня уровень конкурентоспособности в немалой степени зависит от умения защитить свою деловую и техническую информацию от хищений, несанкционированного использования, изменения или уничтожения.

Хорошая идея ценнее кошелька, набитого золотом, а украсть ее легче. Поэтому промышленный шпионаж приобрел поистине гигантский размах.

По оценке экспертов, ежегодный урон американского бизнеса от кражи производственных и торговых секретов превышает четыре миллиарда долларов.

Кроме прямого похищения, происходит и утечка информации, при этом наиболее вероятными ее источниками являются:

- персонал, имеющий доступ к информации;
- документы, содержащие эту информацию;
- технические средства и системы обработки информации, в том числе линии связи, по которым она передается.

Персонал - один из главных каналов утечки информации. Зная это, следует более тщательно изучать биографии особо важных сотрудников. Следует обратить пристальное внимание как на вновь пришедших на работу, так и на тех, кто подлежит увольнению. Эти люди находятся в ситуации, наиболее благоприятной для утечки информации.

Утечка информации - неконтролируемый выход охраняемых сведений за пределы организации или круга лиц, которым они были доверены.

Утечка информации охватывает широкий круг различных действий. Это и утрата информации из компьютера, и пропажа документов. Утратой считается и тайное копирование информации конфиденциального характера с дискеты на дискету, снятая лично для себя копия документа, содержащего тайну. Когда у людей возникает страх перед потерей работы, тогда возможность утечки фирменных секретов утраивается.

Одновременно с понятием (утечка) в законодательных актах применяются и такие как разглашение и несанкционированный доступ к конфиденциальной информации.

Разглашение - сообщение, передача, предоставление, пересылка, опубликование, утеря и оглашение любыми иными способами конфиденциальной информации лицам и организациям, не имеющими права доступа к охраняемым секретам.

Несанкционированный доступ к информации - преднамеренные, противоправные действия злоумышленников с целью получения охраняемых сведений.

Анализируя зарубежный опыт по созданию механизма защиты коммерческой тайны, можно выделить основные блоки, из которых он состоит:

- нормы права, направленные на защиту интересов ее владельцев;
- нормы, устанавливаемые руководством предприятия, фирмы (приказы, распоряжения, инструкции);
- специальные структурные подразделения, обеспечивающие соблюдение этих норм (подразделение режима службы безопасности и т.п.).

Все вышеперечисленное должно быть тесно связано между собой. Так, например, фирма может иметь самые совершенные правила и инструкции, касающиеся внутреннего порядка обращения с конфиденциальными материалами, но при отсутствии государственно-правового регулирования вряд ли сможет защитить свои секреты. Точно также вряд ли удастся сохранить секреты при наличии правового регулирования, но в отсутствие профессионалов, которые будут претворять нормы права и инструкции на практике. Ну, а не зная основных направлений защиты секретов, не удастся сохранить свою конфиденциальную информацию даже при наличии государственной поддержки и наличия специального структурного подразделения в штатном расписании.

Сегодня, когда полным ходом идет процесс становления новых хозяйственных форм и отношений, у предприятий возникают проблемы, связанные с необходимостью защиты собственной секретной информации. Предпринимаемые попытки автоматически перенести сложившуюся систему организации защиты государственных секретов в область коммерческой тайны, скорее всего, обречены на провал.

Мировой опыт в области защиты секретов показывает, что чисто административные меры не гарантируют результат, поэтому предприниматели, не отказываясь от административных мер, переходят к совмещению их с активным вовлечением в процесс защиты конфиденциальной информации всех сотрудников фирмы.

Главное место в организации надежной защиты секретной информации должно отводиться работе с кадрами. Специалисты считают, что сохранность секретов на 80% зависит от правильного подбора, расстановки и воспитания кадров. И эта работа должна начинаться со дня приема человека на работу.

Вторым по важности мероприятием должно быть ограничение доступа к секретной информации. Работа должна быть организована таким образом, чтобы каждый сотрудник имел доступ только к той информации, которая необходима ему в процессе выполнения прямых служебных обязанностей. Эта мера не сможет сама по себе полностью защитить от возможной ее утечки, но позволит свести возможный ущерб к минимуму.

Третьим направлением в работе с персоналом является проведение воспитательной работы. Специалисты в области противодействия промышленному шпионажу дают следующие рекомендации:

- использовать любую возможность для пропаганды программ обеспечения режима секретности;
- всемерно стимулировать заинтересованность сотрудников в выполнении режима секретности;
- не забывать периодически вознаграждать сотрудников за успехи в защите

секретной информации.

- следует иметь в виду, что голые призывы не дают положительных результатов, поэтому значительное место в воспитательной работе необходимо отводить обучению, целями которого являются:
- четкое знание сотрудниками объема охраняемой информации, за безопасность которой он несет личную ответственность;
- понимание исполнителем секретных работ характера и ценности данных, с которыми он работает;
- обучение правилам хранения и защиты секретных данных.

При этом ни одно правило или процедура не должны вводиться без разъяснения их сути, их разумности и необходимости. Каждый руководитель, доводя такие правила до сведения своих подчиненных, обязан подчеркнуть, что они являются неотъемлемой частью их работы.

Вместе с тем не следует ограничиваться только воспитательной работой и обучением. Сотрудник, нарушивший правила работы с секретной информацией, должен знать, что у него будут серьезные неприятности и он будет строго наказан руководством.

Такие подходы к работе с персоналом дают неплохие результаты и могут применяться на фирмах и предприятиях разного профиля деятельности.

Как показывает практика, значительная утечка коммерческой информации происходит в ходе ведения переговоров. Это объясняется разными причинами: неверно понимаемый престиж, неумение правильно рекламировать свою продукцию и т.д. Большую роль играет и умение ведения переговоров. Сотрудник должен четко знать, какую информацию он имеет право сообщить партнеру по переговорам, а какую - нет.

Необходимо учить проведению рекламы по методу "черного ящика", т.е. можно сообщить, например, параметры изделия, полученный результат, а как он получен - секрет фирмы. Сотрудник должен понимать, что от успешно проведенных переговоров зависит не только процветание фирмы, но и его личное благополучие.

Ключевая роль в структуре подразделения, занимающегося защитой коммерческой тайны, должна отводиться аналитической службе. Современное предприятие, функционирующее в условиях рыночной экономики, разумеется, не может позволить себе засекречивать всю информацию. Это слишком дорого и невыгодно: определенная часть сведений должна использоваться в рекламе, к тому же большое количество засекреченных материалов создает помехи в работе.

Вообще существует большое количество способов получения информации. Так, американский журнал “Chemical engineering” опубликовал такой перечень из 16 источников получения информации.

- сбор информации, содержащейся в средствах массовой информации, включая официальные документы, судебные отчеты;
- использование сведений, распространяемых служащими конкурирующих фирм;
- биржевые документы и отчеты консультантов; финансовые отчеты и документы, находящиеся в распоряжении маклеров; выставочные экспонаты и проспекты, брошюры конкурирующих фирм; отчеты коммивояжеров своей фирмы;

- изучение продукции конкурирующих фирм; использование данных, полученных во время бесед со служащими конкурирующих фирм (без нарушения законов);
- замаскированные опросы и “выуживание” информации у служащих конкурирующих фирм на научно-технических конгрессах (конференциях, симпозиумах);
- непосредственное наблюдение, осуществляемое скрытно;
- беседы о найме на работу со служащими конкурирующих фирм (хотя опрашивающий вовсе не намерен принимать данного человека в свою фирму);
- так называемые “ложные” переговоры с фирмой-конкурентом относительно приобретения лицензии;
- наем на работу служащего конкурирующей фирмы для получения требуемой информации;
- подкуп служащего конкурирующей фирмы или лица, занимающегося ее снабжением;
- использование агента для получения информации на основе платежной ведомости фирмы-конкурента;
- подслушивание переговоров, ведущихся в фирмах-конкурентах;
- перехват телеграфных сообщений;
- подслушивание телефонных разговоров;
- кража чертежей, образцов, документации;
- шантаж и вымогательство.

В связи с этим необходимо определить – какая информация должна быть отнесена к коммерческой тайне и требует защиты, каков срок ее “хранения” в качестве тайны, какие ее части наиболее важны. Важность информации определяется ее ценностью для предпринимателя, которая, по мнению ряда специалистов, должна включать полезность (создание субъекту выгодных условий для принятия оперативного решения и получения эффективного результата), своевременность, достоверность и полноту.

Прежде чем приступить к определению информации, относящейся к категории коммерческой тайны, предприниматель должен учесть, что вся имеющаяся информация по степени конфиденциальности, утрата которой может вызвать различные по тяжести последствия, может быть распределена по следующим группам:

Высшая степень конфиденциальности. Данная информация является ключевой в деятельности фирмы, основой ее нормального функционирования. Утрата или разглашение этой информации нанесет непоправимый ущерб деятельности фирмы. Это угроза высокой степени тяжести, последствия реализации которой могут ликвидировать саму фирму.

Строго конфиденциальная информация. Утечка этой информации может вызвать значительные по тяжести последствия. Это информация о стратегических планах фирмы, о перспективных соглашениях и т.п.

Конфиденциальная информация. Ее разглашение наносит фирме ущерб, сопоставимый с текущими затратами фирмы, ущерб может быть преодолен в сравнительно короткие сроки.

Информация ограниченного доступа. Ее утечка оказывает незначительное негативное воздействие на экономическое положение фирмы (должностные инструкции, структура управления).

Открытая информация. Ее распространение не представляет угроз экономической безопасности фирмы. Наоборот, отсутствие данной информации может оказать негативное воздействие на экономическое положение фирмы.

Каким же образом можно осуществить разграничение информации открытой и той, которая нуждается в защите? Для этого следует использовать следующие критерии.

Во-первых, это вероятность угрозы экономической безопасности фирмы. В случае получения этой информации конкурентами фирма понесет экономический ущерб. Так, широко известный напиток “кока-кола” производится на основе секретной формулы, являющейся коммерческой тайной, и обеспечивает процветание фирмы. В случае разглашения этой информации фирму ожидают серьезные экономические трудности.

Во-вторых, это возможность защиты информации. Если, например, информация не входит в обязательный перечень открытого характера, то следует определить - существует ли возможность ее защиты с помощью общих, либо специальных мер защиты.

В-третьих, это экономическая целесообразность защиты информации. Только в том случае, если разглашение или утечка информации может нанести существенный экономический ущерб фирме, следует организовывать ее защиту.

По функционально-целевому признаку выделяются следующие составляющие коммерческой тайны, которые представлены в таблице 3.4.

Как правило, именно перечисленная выше информация в наибольшей степени интересует конкурентов, партнеров, банки, криминальные структуры.

Приведенные направления охватывают практически все аспекты деятельности предприятия, фирмы или компании. И попытаться защитить коммерческую тайну, накладывая ограничения на доступ к информации по перечисленным направлениям, вряд ли возможно, но оказывать противодействие соперникам по конкурентной борьбе на рынке просто необходимо. Вот здесь-то аналитические подразделения и должны сыграть свою роль в определении ключевой информации, выявлении возможных каналов утечки, поиске путей ее защиты. Объективные потребности фирмы, банка, страховой компании и т.п. в обеспечении сохранности тайны определяются рядом факторов, а именно:

- обострением конкурентной борьбы на рынке товаров и услуг; важностью сохранения секретной информации в течение определенного времени;
- возможностью проверить каждый из вероятных каналов утечки информации и в первую очередь по конкретным служащим.

Последние два фактора должны быть тщательно просчитаны по затратам.

3.7 Коммерческая тайна и персонал

В деле защиты предпринимательской деятельности от различного вида угроз значительное место занимает персонал предприятия, который может стать как объектом, так и субъектом таких угроз. Это процесс предполагает проведение превентивных и текущих мер, направленных на работу с кадрами.

Таблица 3.4 – Составляющие коммерческой тайны по функционально-целевому признаку

Деловая информация	- сведения о контрагентах; - сведения о конкурентах; - сведения о потребителях; - сведения о деловых переговорах; - коммерческая переписка; - сведения о заключенных и планируемых контрактах.
Научно-техническая информация	- содержание и планы научно-исследовательских работ; - содержание “ноу-хау”, рационализаторских предложений; планы внедрения новых технологий и видов продукции.
Производственная информация	- технология; - планы выпуска продукции; - объем незавершенного производства и запасов; - планы инвестиционной деятельности.
Организационно-управленческая информация	- сведения о структуре управления фирмой не содержащиеся в уставе; - оригинальные методы организации управления; - система организации труда.
Маркетинговая информация	- рыночная стратегия; - планы рекламной деятельности; - планы обеспечения конкурентных преимуществ по сравнению с продукцией других фирм; - методы работы на рынках; - планы сбыта продукции; - анализ конкурентоспособности выпускаемой продукции.
Финансовая информация	- планирование прибыли, себестоимости; - ценообразование – методы расчета, структура цен, скидки; - возможные источники финансирования; - финансовые прогнозы.
Информация о персонале фирмы	- личные дела сотрудников; - планы увеличения (сокращения) персонала; - содержание тестов для проверки вновь принимаемых на работу.
Программное обеспечение	- программы; - пароли, коды доступа к конфиденциальной информации, расположенной на электронных носителях.

Важность работы с персоналом определяется тем, что в случае желания сотрудника разгласить сведения (в силу корыстных или других мотивов), являющиеся коммерческой тайной, воспрепятствовать этому не смогут никакие, даже дорогостоящие средства защиты.

Угрозы экономической безопасности фирмы со стороны, на, конкурентов, реализуемые через ее персонал, могут принимать такие формы как:

- переманивание сотрудников, владеющих конфиденциальной информацией;
- ложные предложения работы сотрудникам конкурентов с целью выведывания информации;
- выведывание конфиденциальных сведений у сотрудников в такой форме, что последние не догадываются о цели вопросов;
- прямой подкуп сотрудников фирм-конкурентов;
- засылка агентов к конкурентам;
- тайное наблюдение за сотрудниками конкурентов.

На начальной стадии создания фирмы, когда ее штат ограничен несколькими сотрудниками, а финансовые возможности не позволяют осуществить весь комплекс мер по защите информации, складывается ситуация, при которой любые действия конкурентов несут реальную угрозу гибели фирмы. На этой стадии необходимо осуществить хотя бы минимально возможный комплекс мер:

а) предусмотреть, чтобы служащие в заявлениях о приеме на работу, в трудовых соглашениях и контрактах принимали на себя четко выраженные письменные обязательства о неразглашении коммерческой тайны фирмы;

б) определиться с документами, содержащими коммерческую тайну фирмы (сюда относятся прежде всего документы с планами предстоящей деятельности фирмы, технологическая документация, списки поставщиков и покупателей);

в) предусмотреть вопросы защиты коммерческой тайны в типовых соглашениях с заказчиками, покупателями продукции фирмы или ее услуг, продавцами, торговыми агентами и др.

В промышленно развитых странах основой защитой тайны являются законодательные акты и контракты найма-увольнения, заключаемые служащими с фирмой. Даже при наличии соответствующих законов многие фирмы идут на то, чтобы подписывать контракты со своими служащими о неразглашении доверенных им секретов либо с момента установления трудовых отношений, либо когда сотрудник получает доступ к коммерческим секретам.

В наших условиях, когда правового регулирования охраны коммерческой тайны еще не существует, хотя кое-какие проекты уже разработаны, следует обусловить принятие на себя служащими фирмы, работающими по контракту, обязательства о неразглашении коммерческих секретов, при этом данный документ должен прямо предусматривать право работодателя расторгнуть трудовое соглашение (контракт) с сотрудником, нарушившим названное обязательство, а также принимать иные меры, предусмотренные законом.

Конечно, служащий фирмы, подписывая соглашение о неразглашении коммерческой тайны, должен четко представлять, что конкретно из деловой информации и технологических разработок является тайной фирмы. Как раз по этой причине и считается обязательным требование о том, чтобы вся секретная информация была обособлена от остальных сведений, а документы, ее содержащие, носили соответствующую пометку.

На практике для охраны коммерческой тайны фирмы ее служащими как во время работы в ней, так и после увольнения, используются более детально проработанные соглашения. Важно, чтобы условия сохранения коммерческой тайны бывшим сотрудником фирмы были реальными по времени, оставляя ему возможность подыскать достойно оплачиваемую работу.

Использование контрактов о сохранении коммерческой тайны позволяет обеспечить формальную юридическую защиту коммерческой информации, к которой имеет или имел доступ персонал фирмы.

Однако тайны полностью или частично могут стать известны деловым партнерам вашей фирмы в процессе обмена с ними необходимой для совместной работы информацией. Следовательно, они должны принять на себя обязательства по защите ваших коммерческих тайн, равно как и вы должны поступить таким же образом в их отношении. Это традиционная для делового мира практика, но и она

должна подкрепляться письменными обязательствами, т.е. работники должны подписать документ - соглашение о секретности.

Деловые партнеры могут высказать пожелание о предоставлении им всей коммерческой информации для оценки реального состояния ваших дел. На предварительной стадии обсуждения сделки следует воздерживаться от детального обсуждения вашей охраняемой информации. Это возможно лишь после подписания соглашения о сохранении тайны.

Даже тщательно охраняемые тайны фирмы могут стать известны вашим конкурентам из обычных публикаций для широкой публики, если пустить это дело на самотек. Поэтому один из сотрудников должен предварительно просматривать готовящиеся к печати брошюры, рекламные объявления, пресс-релизы и иные материалы, предназначенные для симпозиумов, конгрессов, выставок, а также выступления, научные и иные публикации сотрудников вашей фирмы. Он должен руководствоваться простым, но достаточно эффективным правилом, суть которого состоит в том, чтобы в максимально возможной степени раздробить, разобщить по времени и по авторам ту строго охраняемую коммерческую информацию, без которой невозможно опубликование упомянутых выше работ. Все это существенно препятствует сбору секретной информации о фирме конкурентами или недоброжелателями. Конечно, этот барьер преодолим, но лишь посредством очень больших затрат.

Трудно найти золотую середину между стремлением сохранить коммерческую тайну и желанием использовать в рекламных целях наиболее впечатляющие данные из строго охраняемой информации, особенно те из них, которые, несомненно, помогли бы расширить сбыт производимых товаров и услуг.

Где и как предприниматель может получить необходимые ему сведения о клиентах и конкурентах, дающие ему возможность нормально работать в условиях рыночной экономики? Известно, что обладание такими сведениями по сути своей есть один из элементов системы превентивных мер по борьбе с промышленным шпионажем.

В капиталистических странах сведения о клиентах принято считать не коммерческой тайной фирмы, а, скорее, ее капиталом. Поэтому список клиентов фирмы и иные сведения о них составляются, в первую очередь, усилиями руководителя и эта информация не доверяется даже его ближайшему окружению.

Сведения о деятельности фирмы и ее руководителях собирают в различных экономических газетах и журналах, справочниках, выпытывают у биржевиков, покупают у частных детективов.

Осведомленность о наиболее выгодных клиентах конкурента дает шанс победить в состязании с ним, если вам удастся "переманить" его клиентуру. Здесь на первый план выступает персонифицированная информация о клиентах, сведения о симпатиях и антипатиях, об их привязанностях, дружеских связях в среде предпринимателей и их конкурентах, которые влияют на принятие ими решений о поддержке деловых отношений с вашей фирмой или об их прекращении.

Сбор информации о клиентах и конкурентах должен быть упорядочен самым тщательным образом, и эта информация должна находиться только у руководства фирмы.

Сотрудники фирмы, продвигающие на рынок ее продукцию, должны представить письменные отчеты о конкретных клиентах по каждому факту продаж. В этих отчетах должны быть отражены перспективы будущих сделок.

Если вашей фирме по силам затраты на содержание аналитического отдела, изучающего конъюнктуру рынка, клиентов, конкурентов, то и в этом случае следует дозировано распределять такого рода конфиденциальную информацию среди сотрудников.

Документация об этом должна быть строго секретной, а персонал, работающий с ней, должен соблюдать правила обращения с секретными документами. Все служащие, работающие непосредственно с клиентами, должны дать письменные обязательства сохранять коммерческие тайны фирмы.

Аналитический отдел или отдел маркетинга, изучая клиентов, должен одновременно собирать и анализировать сведения о конкурентах. Для этого должна быть разработана программа действий каждого сотрудника отдела. Следует четко знать, какие сведения надо получить и где они концентрируются. Кто и каким образом может получить эти сведения с наименьшими затратами. Какие трудности могут возникнуть при этом, и как их следует преодолевать. Обязательно следует фиксировать: где, когда и как получена данная информация, кем конкретно и что по ней сделано.

В наших условиях добывание достоверной информации о клиентах и конкурентах - предмет постоянной головной боли. Рынок, его информационные структуры находятся еще в стадии формирования, притом на самых первых ступенях. По этой причине решение проблемы, вероятнее всего, может осуществляться:

- собственными силами (создание отделов маркетинга, изучения спроса и т.д.);

- получением за плату нужной информации у тех коммерческих структур, которые ею располагают (банки, страховые компании, биржи, частные детективные агентства и т.п.);

- обращением за помощью, разумеется, платной, к службам промышленной контрразведки, к частным сыскным агентствам и т.д.

Предприниматель осуществляет выбор сам, но в любом случае выбор этот потребуется сделать, потому что система превентивных мер, обеспечивающая безопасность фирмы, без исчерпывающей информации о ее клиентах и конкурентах существовать не может, а сама фирма в таких условиях обречена на проигрыш в конкурентной борьбе.

Добывая жизненно важную коммерческую информацию, не следует забывать, что ваши конкуренты озабочены тем же. Во Франции, например, за промышленными секретами охотятся десятки тысяч промышленных шпионов и на оплату их труда французские бизнесмены ежегодно тратят свыше одного миллиарда долларов.

Не следует забывать о работе с представителями средств массовой информации, тем более что наше законодательство никак не защищает предпринимателей от журналистов.

Закон о печати не предусматривает ответственность за возможность нанесения публикацией даже существенного имущественного вреда посредством разглашения коммерческих тайн предпринимателей.

Столь существенные недочеты Закона "О средствах массовой информации", не говоря уже о других менее значимых, заставляют (и обязывают!) любого предпринимателя быть настороже при общении с журналистами. Вообще-то, следует исходить из известного правила: минимум информации - максимум общественного интереса.

3.8 Банковская тайна

Одной из специфических разновидностей коммерческой тайны является банковская тайна.

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

Банки, как правило, работают с многочисленными клиентами, вкладчиками, корреспондентами, интересы которых могут пострадать при разглашении информации об их операциях, сделках, счетах и пр. Причем угрозы могут исходить как от конкурентов, так и от преступных сообществ. В связи с этим возникает необходимость в защите информации, которой обладают банки, в том числе и информации о деятельности лиц, пользующихся разнообразными услугами банков.

Особенность правового режима банковской тайны заключается в том, что перечень сведений, включаемых в нее, устанавливается не только законодательно, но и самими банками. Причем, в Российской Федерации пока нет отдельного закона о банковской тайне, а законодательное регулирование осуществляется в основном Гражданским кодексом РФ и Федеральным законом “О банках и банковской деятельности”. В этих законодательных актах предусмотрено, что банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиентах и корреспондентах. Кроме того, банки сами могут относить часть информации, которой они владеют к категории банковской тайны (если это не противоречит федеральному закону). Служащие банка обязаны хранить банковскую тайну.

Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом. Закон же предусматривает, что справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, органам государственной налоговой службы и налоговой полиции, таможенным органам Российской Федерации в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия прокурора – органам предварительного следствия по делам, находящимся в их производстве. Справки по счетам и вкладам в случае смерти их владельцев выдаются кредитной организацией лицам, указанным владельцем счета или вклада в сделанном кредитной организации завещательном распоряжении, нотариальным конторам по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан – иностранным консульским учреждениям.

Коммерческие банки тесно связаны с Банком России, который получает от них большое количество информации. Законодательно установлено, что Банк России не вправе разглашать информацию о счетах, вкладах, конкретных сделках и об операциях из отчетов кредитных организаций, полученных им в результате исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Кроме того, аудиторские организации, осуществляющие обязательные ежегодные проверки кредитных организаций, также не вправе раскрывать третьим лицам сведения об операциях, о счетах и вкладах кредитных организаций, их клиентов и корреспондентов, полученные в ходе проводимых ими проверок, за исключением случаев, предусмотренных федеральными законами.

За разглашение банковской тайны Банк России, кредитные, аудиторские и иные организации, а также их должностные лица и работники несут ответственность, включая возмещение нанесенного ущерба, в порядке, установленном федеральным законом. Гражданско-правовая ответственность выражается в применении способов защиты гражданских прав, предусмотренных ст. 12 ГК РФ. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных ему убытков.

Несмотря на наличие ряда общих законодательных норм, гарантирующих сохранение банковской тайны, в российском законодательстве отсутствует разъяснение того, что понимается под этой гарантией, какие условия должны при этом выполняться, каковы критерии обеспечения защиты информации, составляющей банковскую тайну и т. п. В связи с этим, реальное обеспечение защиты банковской тайны в современных условиях сопряжено со значительными трудностями.

В нынешних условиях угрозы банковской тайны зачастую исходят не только от конкурентов и преступных группировок, но и от правоохранительных органов, например, налоговой полиции. Злоупотребления в этом случае могут иметь форму:

- изъятия конфиденциальных документов без надлежащего правового оформления (протокола выемки);
- проведения обыска без санкции прокурора;
- использования спецсредств (“жучков”) в собственных корыстных целях и др.

Вопросы для повторения темы:

1. Дайте определение конфиденциальной информации и коммерческой тайны. В чем сходство и различие этих двух понятий?
2. Верно ли на Ваш взгляд утверждение: Предприятие может самостоятельно устанавливать перечень документов с грифом «коммерческая тайна»?
3. Что Вы понимаете под угрозой целостности данных?
4. В какой части документа проставляется гриф ограничения доступа?
5. Назовите основные стадии жизненного цикла документа.
6. В чем заключается «политика чистых столов»?
7. Какие правила следует соблюдать при работе с документами, содержащими коммерческую тайну?

8. Какие принимаются меры в случае утери документа, составляющего коммерческую тайну?

9. На какие два типа делятся телефонные радиомикрофоны? В чем преимущества и недостатки каждого типа?

10. Перечислите основные средства превентивной защиты информации.

11. Раскройте суть метода «инверсия спектра».

12. Чему на Ваш взгляд следует уделять внимание в первую очередь при защите секретной информации?

13. На какие группы делится информация по степени конфиденциальности?

14. На основе каких критериев осуществляется разграничение информации на открытую и закрытую?

15. Каким основным правилом следует руководствоваться, когда необходимо раскрыть в СМИ информацию, относящуюся к коммерческой тайне?

16. Дайте определение банковской тайне.

Литература:

1. Веснин В.Р. Технология работы с персоналом и деловыми партнерами. – М.: «Элит-2000», 2002.- 592с.

2. Галатенко В.А. Основы информационной безопасности. Курс лекций. Учебное пособие. – М.: «Институт», 2003.- 280с.

3. Соболев А.Н. Физические основы технических средств обеспечения информационной безопасности. – М.: «Гелиос АРВ», 2004.- 224с.

4. Степанов Л.Я. Управление персоналом: персонал в системе защиты информации. – М.: «Инфра-М», 2002.- 288с.

5. Уфимцев Ю.С. Методика информационной безопасности. Монография. – М.: «Экзамен», 2004. – 544с.

Глава 4 Компьютерная безопасность

Ключевые понятия:

Компьютерные преступления
Компьютерная информация
Операционные преступления
"Взлом" изнутри
"Взлом" извне
Фоун-фрейкинг
Уивинг
Маршрутизатор
Правовое обеспечение
Организационное обеспечение
Программно-техническое обеспечение
Аппаратные средства защиты
Программные средства защиты
Криптография
Симметричное шифрование
Асимметричное шифрование
Необратимое шифрование

4.1 Общие положения

Первый зарегистрированный случай злоупотребления с использованием компьютера относится к 1958 году.

Первое преступление с использованием компьютера в бывшем СССР было зарегистрировано в 1979 г. в Вильнюсе. Ущерб государству от хищения составил

78,5 тыс. рублей. Данный факт был занесен в международный реестр правонарушений подобного рода и явился своеобразной отправной точкой в развитии нового вида преступлений в нашей стране.

Термин "**компьютерная преступность**" впервые появился в американской, а затем другой зарубежной печати в начале 60-х годов. В 1983 году в Париже группой экспертов ОЭСР было дано криминологическое определение **компьютерного преступления**, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных и (или) передачу данных.

Компьютерные преступления – это преступления в сфере компьютерной информации, а также преступления, совершаемые с использованием компьютерных технологий.

Компьютерная информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, хранящихся в компьютерной системе, сети или машинных носителях.

К наиболее типичным целям совершения компьютерных преступлений специалисты относят следующие:

- подделка отчетов и платежных ведомостей;
- приписка сверхурочных часов работы;
- фальсификация платежных документов;
- хищение из денежных фондов;
- добывание запасных частей и редких материалов;
- кража машинного времени;
- вторичное получение уже произведенных выплат;
- фиктивное продвижение по службе;
- получение фальшивых документов;
- внесение изменений в программы и машинную информацию;
- перечисление денег на фиктивные счета;
- совершение покупок с фиктивной оплатой и др.

В своих преступных деяниях компьютерные преступники руководствуются следующими основными мотивами:

1. Выйти из финансовых затруднений;
2. Получить, пока не поздно, от общества то, что оно якобы задолжало преступнику;
3. Отомстить фирме и работодателю;
4. Выразить себя, проявить свое "я";
5. Доказать свое превосходство над компьютерами.

Отличительными особенностями данных преступлений являются:

- высокая латентность,
- сложность сбора доказательств,
- транснациональный характер (как правило, с использованием телекоммуникационных систем),
- значительность материального ущерба,
- специфичность самих преступников (как правило, ими являются высококвалифицированные программисты, банковские служащие).

Высокая латентность компьютерных преступлений обусловлена тем, что многие организации разрешают конфликт своими силами, поскольку убытки от

расследования могут оказаться выше суммы причиненного ущерба (изъятие файлового сервера для проведения экспертизы может привести к остановке работы на срок до двух месяцев, что неприемлемо ни для одной организации). Их руководители опасаются подрыва своего авторитета в деловых кругах и в результате - потери большого числа клиентов, раскрытия в ходе судебного разбирательства системы безопасности организации, выявления собственной незаконной деятельности.

Компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. По данным ООН, уже сегодня ущерб, наносимый компьютерными преступлениями, сопоставим с доходами от незаконного оборота наркотиков и оружия. Только в США ежегодный экономический ущерб от такого рода преступлений составляет около 100 млрд. долл. Причем многие потери не обнаруживаются или о них не сообщают.

По данным недавнего исследования Института компьютерной безопасности, в котором приняли участие представители 250 компаний, убытки от компьютерных преступлений (как внутренних, так и внешних) в 2003 году составили в общей сложности 137 млн. долл., что на 37% больше по сравнению с 2002 годом.

Наибольшую опасность представляет компьютерная преступность в финансовой сфере. Отмечается тенденция к росту компьютерных преступлений в банковской сфере. Согласно результатам независимых опросов, проведенных социологической службой "Кассандра", каждый второй респондент спрогнозировал рост банковских убытков из-за возрастания вероятности мошенничества.

4.2 Субъекты компьютерных преступлений

Лица, совершающие компьютерные преступления, могут быть объединены в три большие группы:

1. Лица, не связанные трудовыми отношениями с организацией жертвой, но имеющие некоторые связи с нею;
2. Сотрудники организации, занимающие ответственные посты;
3. Сотрудники пользователи ЭВМ, злоупотребляющие своим положением.

Специалисты подразделяют представляющий опасность персонал на категории в соответствии со сферами деятельности

Операционные преступления - совершаются операторами ЭВМ, периферийных устройств ввода информации в ЭВМ и обслуживающими линии телекоммуникации.

Преступления, основанные на использовании программного обеспечения, обычно совершаются лицами в чьем ведении находятся библиотеки программ; системными программистами; прикладными программистами; хорошо подготовленными пользователями

Для аппаратурной части компьютерных систем опасность совершения преступлений представляют:

- инженеры системщики;
- инженеры по терминальным устройствам;
- инженеры-связисты;
- инженеры-электронщики.

Определенную угрозу совершения компьютерных преступлений представляют и сотрудники, занимающиеся организационной работой:

- управлением компьютерной сетью;
- руководством операторами;
- управлением базами данных;
- руководством работой по программному обеспечению.

Определенную угрозу могут представлять также разного рода клерки, работники службы безопасности, работники, контролирующие функционирование ЭВМ.

Особую опасность могут представлять специалисты в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются.

Около 90% злоупотреблений в финансовой сфере, связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих или бывших работников банков. При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории банковских служащих - системные администраторы и другие сотрудники служб автоматизации банков.

4.3 Классификация компьютерных преступлений

В зависимости от способа воздействия на компьютерную систему специалисты выделяют четыре вида компьютерных преступлений:

- **Физические злоупотребления**, которые включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.
- **Операционные злоупотребления**, представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование различных устройств.
- **Программные злоупотребления**, которые включают в себя: различные способы изменения системы математического обеспечения ("логическая бомба" - введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; "троянский конь" - включение в обычную программу своего задания).
- **Электронные злоупотребления**, которые включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение программы.

Принято классифицировать компьютерные преступления в зависимости от способа их совершения. По мнению большинства специалистов, все способы совершения компьютерных преступлений можно объединить в три основные группы (Таблица 4.1).

При совершении ряда преступлений могут иметь место все три способа использования компьютера.

Рассмотрим каждый из видов более подробно.

1. Компьютер как объект преступления. Можно выделить две разновидности преступлений, где компьютер является объектом посягательства:

а) изъятие средств компьютерной техники. К этой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества.

б) атака на компьютер с целью несанкционированного доступа в целях получения доступа к хранящейся на нем информации (хищения информации), бесплатного использования данной системы (кража услуг) или ее повреждения.

Большинство таких нарушений предполагают несанкционированный доступ к системе, т.е. ее "взлом". В общем виде используемые компьютерными преступниками методики несанкционированного доступа сводится к двум разновидностям:

"Взлом" изнутри: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля.

Таблица 4.1 - Классификация компьютерных преступлений в зависимости от способа их совершения

1. Методы перехвата	
а) Непосредственный перехват	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.
б) Электромагнитный перехват	Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д., может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.
2. Методы несанкционированного доступа	
а) Следование "За дураком"	Имеет целью несанкционированное проникновение в пространственные и 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.
б) "За хвост"	Используя этот метод, можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.
в) "Компьютерный абордаж"	Обычно используется для проникновения в чужие информационные сети. Злоумышленник пытается с помощью автоматического перебора абонентских номеров соединиться с тем или иным компьютером, подключенным к телефонной сети. Делается это до тех пор, пока на другом конце линии не отзовется другой компьютер. После этого достаточно подключить собственный компьютер. Угадав код можно внедриться в чужую информационную систему.
г) "Неспешный выбор"	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.
д) "Поиск бреши"	Данный метод основан на использовании ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно.

Продолжение Таблицы 4.1

2. Методы несанкционированного доступа	
е) "Люк"	Является развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется необходимое число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу.
ж) "Маскарад"	В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя.
з) "Мистификация"	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.
и) "Аварийный"	Этот прием основан на использовании того обстоятельства, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ.
к) "Склад без стен"	Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных.
3. Методы манипуляции (сущность методов манипуляции состоит в подмене данных, которая осуществляется, как правило, при вводе-выводе данных, это простейший и потому очень часто применяемый способ)	
а) "Троянский конь"	Способ, состоящий в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе либо оказать воздействие на администрацию предприятия с корыстной целью.
б) "Логическая бомба"	Тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.
в) "Временная бомба"	Разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.
г) "Асинхронная атака"	Состоит в смешивании команд двух или нескольких пользователей, чьи команды компьютерная система выполняет одновременно.
д) Реверсивная модель	Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе, прокручивание модели "вперед-назад" может проходить не один раз, чтобы через несколько итераций добиться желаемого.
е) "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 до тех пор, пока на счете не оказывается приличная сумма. Тогда деньги быстро снимаются и владелец счетов скрывается.

"Взлом" извне: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий. В данной категории преступлений выделяют также:

а) преступления, совершаемые в отношении компьютерной информации, находящейся в компьютерных сетях, в том числе сети Интернет;

б) преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.).

Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путем "взлома" защитных систем организаций.

4.3.1 Хищение информации

Правонарушения, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ. Информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырех типов:

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;
- объекты интеллектуальной собственности и материалы, защищенные авторским правом;
- глобальная информация, имеющая значение для развития отраслей промышленности, экономики отдельных регионов и государств.

Похищаются сведения об новейших научно-технических разработках, планах компании по маркетингу своей продукции и заключаемых сделках.

Предметом хищения может быть также другая экономически важная информация, в частности, реквизиты банковских счетов и номера кредитных карточек.

Можно выделить два основных направления действий преступников:

- электронная атака на узловые серверы и броузеры сети WWW в целях перехвата информационных потоков;
- поиск в защитных системах локальных компьютерных сетей уязвимых мест и проникновение в базы данных с целью съема находящейся в них информации.

4.3.2 Хищение услуг

К данной группе правонарушений относится получение несанкционированного доступа к какой-то системе, чтобы бесплатно воспользоваться предоставляемыми ею услугами.

Примером преступления данной категории является фоун-фрейкинг.

Фоун-фрейкинг – использование компьютера для проникновения в коммутационную телефонную систему с целью незаконного пользования услугами по предоставлению междугородной телефонной связи.

Сюда же можно отнести использование ресурсов систем - объектов несанкционированного доступа для решения задач, требующих сложных расчетов, например, для определение закодированных паролей, которые они похищают с других узлов.

Уивинг - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы.

4.3.3 Повреждение системы

Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы - объекта несанкционированного доступа. Данная деятельность осуществляется по трем основным направлениям:

1. Проводится массированная подача электронных сигналов на серверы WWW и локальных сетей в целях вывода их из строя, для чего используются специально разработанные программы.
2. В базы данных ЭВМ и корпоративных сетей вводятся вирусы-роботы, которые в заданный момент искажают или уничтожают компьютерные файлы.
3. Манипуляция данными.

Объектом подобных атак могут стать компьютеры, соединенные с Интернетом.

Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.

4.3.4 Использование вирусов

Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающих лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания.

Не представляет сложности купить CD-диски с программами взлома систем защиты компьютерных сетей, а также CD-диски с пакетами вирусов, которые можно использовать для заражения средств вычислительной техники. Также продается специальная программа-конструктор для генерации вирусов. С ее помощью даже не специалист может создать штамм вируса из готовых стандартных составных частей различных вредоносных программ. Причем каждый новый вирус, сгенерированный программой-конструктором, не определяется антивирусом, пока его копия не попадет к авторам антивирусных программ. Таким образом, в пользование различных лиц свободно попадают вирусные программы, а также программы-конструкторы по их созданию, что может привести к тяжелым последствиям.

Особую опасность представляют злоупотребления, связанные с распространением вирусов через Интернет.

4.3.5 Компьютер как орудие преступления

Компьютеры могут использоваться в качестве орудия незаконных действий двояким способом:

а) как средство совершения традиционных преступлений (различного рода мошенничества и т.п.);

б) как средство атаки на другой компьютер.

Компьютер как орудие совершения обычных преступлений. Значительная часть преступлений данной категории совершается с использованием Интернет. К ним относятся: мошенничество с предоплатой; пирамиды и письма по цепочке; виртуальные финансовые пирамиды и ряд других.

Компьютер как средство атаки на другие компьютеры. В некоторых случаях компьютер может одновременно являться объектом несанкционированного доступа и средством атаки. Однако в большинстве случаев атаки на компьютеры совершаются с других компьютеров, находящихся в той же сети. Поскольку такие сети состоят из сотен или тысяч узлов на многих континентах, соответственно существует больше возможностей для несанкционированного доступа или других нарушений.

Существует две основных категории дистанционных нарушений:

- несанкционированный доступ;
- отказ в обслуживании.

При нарушении с несанкционированным доступом преступник пытается воспользоваться пробелами в области обеспечения безопасности системы в качестве средства для получения доступа к самой системе. Если ему это удается, он может похитить или уничтожить информацию или использовать поврежденную систему в качестве платформы, с которой он сможет совершить нарушения в отношении других машин. Значительной опасностью характеризуются подобные злоупотребления в Интернет.

При нарушении, влекущем за собой отказ в предоставлении обслуживания, цель преступника состоит в выведении из строя данной системы. При этом преступник не обязательно стремится получить к ней доступ. Наибольшее распространение получили подобные нарушения в сети Интернет.

4.3.6 Компьютер как запоминающее устройство

В данной своей функции компьютер играет в преступной деятельности роль пассивного запоминающего устройства. Часто при этом компьютер является объектом несанкционированного доступа.

Например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек.

Таблица 4.2, составленная по результатам опроса представителей служб безопасности 492 компаний в 2003г., дает представление о наиболее опасных способах совершения компьютерных преступлений (допускалось несколько вариантов ответов).

Таблица 4.2 – Способы совершения компьютерных преступлений

Угроза	Выявление за последние 12 месяцев
Вирус	83%
Злоупотребление сотрудниками компании доступом к Internet	69%
Кража мобильных компьютеров	58%
Неавторизованный доступ со стороны сотрудников компании	40%
Мошенничество при передаче средствами телекоммуникаций	27%
Кража внутренней информации	21%
Проникновение в систему	20%

4.4 Контроль над компьютерной преступностью

Меры контроля над компьютерной преступностью подразделяются на:

- правовые;
- организационное;
- программно-технические.

4.4.1 Правовые меры

К правовым мерам относятся разработка норм, устанавливающих ответственность за совершение компьютерных преступлений, защита авторских прав программистов, а также вопросы контроля за разработчиками компьютерных систем и применение международных договоров об их ограничениях.

Правовое обеспечение - это совокупность норм права, определяющих общественные отношения, которые возникают в процессе деятельности людей по безопасному использованию компьютерной техники для обработки информации.

Эти правовые нормы могут быть представлены в виде законов, положений, инструкций, руководств, иных нормативно-правовых документов (законодательных актов в информационно сфере, документов, регулирующих общесистемные требования, различные виды стандартов).

Правовое обеспечение информационной безопасности означает:

- защиту интересов государства;
- защиту интересов юридических и физических лиц.

Правовое обеспечение компьютерной безопасности включает следующие виды деятельности:

- нормотворческая деятельность по созданию законодательства, регулирующего отношения в обществе, связанные с обеспечением защиты компьютерной информации;
- исполнительская и правоприменительная деятельность в области защиты компьютерной информации;
- оценка состояния действующего законодательства и разработка программы его совершенствования;

создание организационно-правовых механизмов обеспечения защиты компьютерной информации;

- формирование правового статуса субъектов в системе защиты компьютерной информации.

В РФ основы законодательного регулирования информационных отношений в обществе с учетом мировой практики, современного уровня развития информационных технологий заложены в федеральных законах: «О связи», «Об информации, информатизации и защите информации», «О государственной тайне», «О средствах массовой информации», а также в ряде других нормативных актов на уровне субъекта Федерации и муниципальных образований с учетом их специфики.

4.4.2 Организационное обеспечение

Организационное обеспечение - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий. Организационное обеспечение компьютерной безопасности включает в себя следующие направления (Рисунок 4.1).

Организационно-технические мероприятия по обеспечению компьютерной безопасности предполагают активное использование инженерно-технических средств.

Например, в открытых сетях для защиты информации применяют межсетевые экраны.

Межсетевые экраны - это локальное или функционально-распределительное программно-аппаратное средство, реализующее контроль за информацией, поступающей в компьютер или выходящей из него.

Известно три типа межсетевых экранов:

1) на основе фильтрации пакетов сообщений - анализируют значения полей «адрес» и «порт» в заголовке и на основе заранее определенных правил пропускают либо отклоняют порт. Характеризуются простотой, дешевизной, малым влиянием на производительность сети.

2) на основе технологии контекстной проверки - просматривают пакеты на сетевом уровне и анализируют некоторые данные в пакете по отношению к применяемым сервисам.

3) на основе технологии «посредника» - являются промежуточным звеном передачи пакетов между сервером и клиентом.

Организационное обеспечение.

Для организации взаимодействия с Internet рекомендуется создание отдельного Internet-сегмента, таким образом, типовой сегмент Internet организации состоит из двух относительно самостоятельных частей;

1. Открытого Internet-сегмента, включающего общедоступный WEB-сервер, внешний DNS-сервер, FTP-сервер, почтовый сервер и другие, предоставляющие необходимые сервисы Internet.

Данный Internet-сегмент подключается к Internet через внешний экранирующий маршрутизатор, запрещающий все виды потоков сообщений (трафика), кроме трафика от прикладного экрана, общедоступных серверов организации к Internet и обратно.

Рисунок 4.1 – Направления организационного обеспечения компьютерной безопасности

2. Внутреннего Internet-сегмента, включающего служебные серверы организации, сервер удаленного доступа, элементы управления компьютером (рабочие станции), персонала организации и др.

Данный сегмент подключается к Internet через внутренний экранирующий маршрутизатор, прикладной экран и внешний экранирующий маршрутизатор.

Прикладной экран размещается между открытым и внешним Internet-сегментами. Он осуществляет фильтрацию пакетов сообщений и обеспечивает разграничение прав доступа к информационным ресурсам по адресу сервера, имени файла, типу команды и др.

4.4.3 Программно-технические меры

К программно-техническим мерам можно отнести:

- защиту от несанкционированного доступа к системе;
- профилактику от компьютерных вирусов;
- резервирование особо важных компьютерных подсистем;
- применение конструктивных мер защит от хищений, саботажа, диверсий, взрывов;
- установку резервных систем электропитания;
- оснащение помещении кодовыми замками;

- установку сигнализации и другие меры.

Программно-техническое обеспечение - совокупность специальных органов, технических средств и мероприятий по их использованию в интересах обеспечения безопасности предприятия. Программно-техническая защита включает в себя:

1. Технические средства защиты компьютерной техники и периферийных устройств;
2. Физические средства защиты (охрана, сигнализация, системы оповещения);
3. Аппаратные, программные и программно-аппаратные средства защиты;
4. Криптографические средства защиты.

Остановимся поподробнее на последних двух компонентах программно-технической защиты компьютерной информации.

Аппаратные средства защиты - это непосредственно встроенные в компьютер системы передачи данных или оборудованные в виде самостоятельных приспособлений устройства, которые служат для внутренней защиты структурных элементов компьютерной техники.

Программные средства защиты - это соответствующие процедуры, входящие в состав программного обеспечения систем обработки данных или самостоятельное программное обеспечение, входящее в состав комплексов и систем аппаратуры контроля.

Наибольшее распространение получили программно-аппаратные средства защиты - комплекс программно-аппаратных средств, к которому в общем случае предъявляются следующие требования:

а) комплексность - использование в разнообразных режимах защищенной обработки данных с учетом возможных действий злоумышленника;

б) совместимость - система защиты не должна ограничивать пользователя в применении какого-либо программного обеспечения;

в) переносимость - иметь предельно малые габариты и вес;

г) удобство в работе - система защиты не должна изменять привычную технологию работы пользователей, снижая тем самым производительность их работы;

д) работа в масштабе реального времени - осуществлять все процессы преобразования информации с достаточно большой скоростью;

е) высокий уровень защиты;

ж) минимально возможная стоимость;

з) простота установки, обслуживания и тиражирования.

В России долгое время достаточно широко применялся и продолжает применяться программно-аппаратный комплекс средств защиты компьютерной информации от несанкционированного доступа «**Аккорд**», состоящий из средств защиты компьютера и средств разграничения доступа к его ресурсам (Рисунок 4.2). Мы рассмотрим этот довольно простой комплекс защиты для дальнейшего понимания принципов остальных программно-аппаратных комплексов.

Подсистема управления доступом предназначена для защиты компьютера от посторонних пользователей, для управления доступом к объектам доступа и организации совместного их применения зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа.

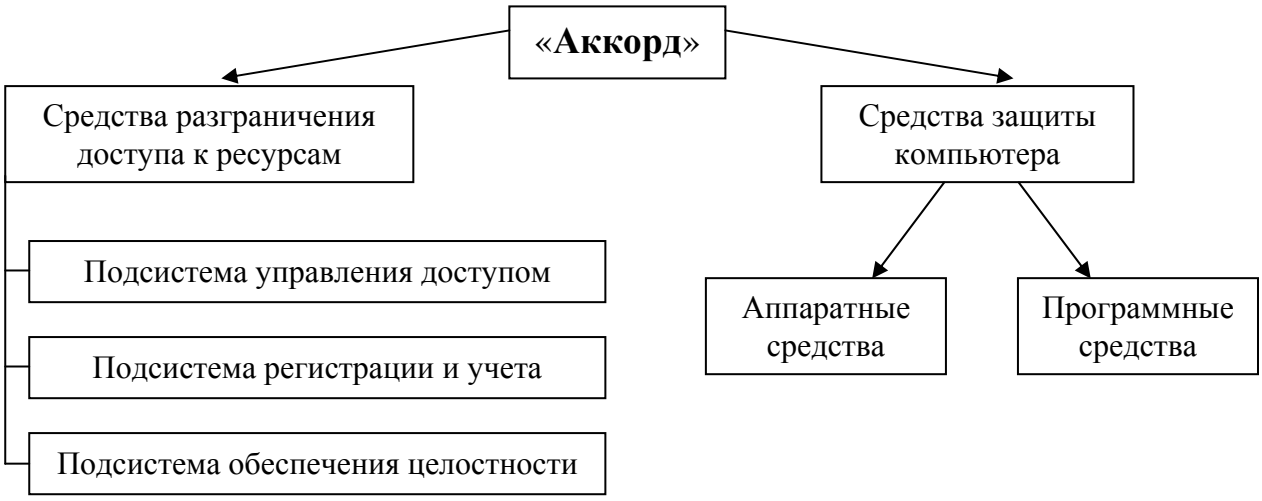

Рисунок 4.2 - программно-аппаратный комплекс средств защиты компьютерной информации от несанкционированного доступа «Аккорд»

Подсистема регистрации и учета предназначена для регистрации в системном журнале событий, происходящих в компьютере.

Подсистема обеспечения целостности предназначена для исключения несанкционированных модификаций (злоумышленных или случайных) программной среды, в том числе программных средств комплекса, а также обрабатываемой информации. Данная подсистема обеспечивает при этом защиту компьютера от внедрения программных закладок и вирусов.

Для обеспечения функционирования названных систем комплекс «Аккорд» включает следующие аппаратные и программные средства:

Аппаратные средства:

- одноплатный контроллер, который устанавливается в свободный слот материнской платы;
- контактное устройство-съемник информации (обычно устанавливается на передней панели компьютера);
- интеллектуальный персональный идентификатор («Touch memory» - память касания).

Программные средства - специальное программное обеспечение разграничения доступа, контроля обращения к ресурсам и регистрации событий (поставляется для конкретной операционной системы).

В качестве персональных идентификаторов в различных программно-аппаратных средствах защиты могут использоваться:

- считыватели штрих-кодов;
- считыватели магнитных карт;
- биометрические считыватели (отпечатки пальца, сетчатка глаза, геометрия ладони руки, тембр голоса, почерк и т.д.)

Криптографические средства защиты - это средства защиты данных при помощи криптографического преобразования, то есть преобразования данных шифрованием.

Криптография - наука, изучающая принципы, средства и методы преобразования данных с целью сокрытия их содержания, предотвращая, таким образом, их несанкционированное использование или скрытую модификацию.

В результате криптографического преобразования получается зашифрованный текст. Различают:

а) **симметричное шифрование** (для шифрования и расшифровки используется один и тот же ключ);

б) **асимметричное шифрование** (для шифрования используется один ключ, для расшифровки - другой);

в) **необратимое шифрование** (используется при шифровании паролей, зашифрованный текст записывается в память, далее сравниваются зашифрованные строки текста, при этом данные не могут быть воспроизведены).

В качестве паролей большинство исследователей не рекомендуют использовать:

- свои Ф. И. О., а также имена и фамилии близких родственников;
- свои номера телефонов;
- номерной знак своего автомобиля;
- пароли, содержащие одинаковые буквы;
- комбинации букв на клавиатуре (qwerty);
- дату рождения (свою, близких родственников, друзей, коллег по работе и др.);
- слова: user, master, guru, got и другие подобные.

4.5 Меры защиты компьютерной безопасности

Для уменьшения ущерба от компьютерного преступления очень важно своевременно его обнаружить. Для того чтобы обнаружить компьютерное преступление или уязвимые места в системе информационной безопасности следует обращать внимание на:

- несанкционированные попытки доступа к файлам данных;
- кражи частей компьютеров;
- кражи программ;
- физическое разрушение оборудования;
- уничтожение данных или программ.

Это только самые очевидные признаки, на которые следует обратить внимание при совершении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление уже совершено, или что не выполняются меры защиты. Они также могут свидетельствовать о наличии уязвимых мест - указать, где находится дыра в защите - и помочь наметить план действий по устранению уязвимого места. В то время как признаки могут помочь предотвратить его.

О наличии уязвимых мест в компьютерной безопасности могут свидетельствовать следующие признаки:

1. Не разработано положений о защите информации или они не соблюдаются. Не назначен ответственный за информационную безопасность.

2. Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, ими делятся с другими, или они появляются на компьютерном экране при их вводе

3. Удаленные терминалы и микрокомпьютеры оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра.

4. Не существует ограничений на доступ к информации, или на характер ее использования. Все пользователи имеют доступ ко всей информации и могут использовать все функции системы.

5. Не ведется системных журналов, и не хранится информация о том, кто и для чего использует компьютер.

6. Изменения в программы могут вноситься без их предварительного утверждения руководством.

7. Отсутствует документация или она не позволяет делать следующее:

а) понимать получаемые отчеты и формулы, по которым получаются результаты;

б) модифицировать программы;

в) готовить данные для ввода;

г) исправлять ошибки;

д) производить оценку мер защиты;

е) понимать сами данные - их источники, формат хранения, взаимосвязи между ними.

8. Делаются многочисленные попытки войти в систему с неправильными паролями.

9. Вводимые данные не проверяются на корректность и точность, или при их проверке много данных отвергается из-за ошибок в них, требуется сделать много исправлений в данных, не делается записей в журналах об отвергнутых транзакциях.

10. Имеют место выходы из строя системы, приносящие большие убытки.

11. Не производился анализ информации, обрабатываемой в компьютере, с целью определения необходимого для нее уровня безопасности.

12. Мало внимания уделяется информационной безопасности. Хотя политика безопасности и существует, большинство людей считает, что на самом деле она не нужна.

С целью защиты информации каждый пользователь должен знать и осуществлять следующие меры:

1. Контроль доступа как к информации в компьютере, так и к прикладным программам. Необходимо иметь гарантии того, что только авторизованные пользователи имеют доступ к информации и приложениям.

2. Нужно требовать, чтобы пользователи выполняли процедуры входа в компьютер, и использовать это как средство для идентификации в начале работы. Чтобы эффективно контролировать компьютер, может оказаться наиболее выгодным использовать его как однопользовательскую систему.

3. Необходимо использовать уникальные пароли для каждого пользователя, которые не являются комбинациями данных пользователей, для аутентификации личности пользователя. Нужно внедрить меры защиты при администрировании паролей и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению.

4. Процедуры авторизации. Необходимо разработать процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям и предусмотреть соответствующие меры по внедрению этих процедур в организации. Также установить порядок в организации, при котором для использования компьютерных ресурсов, получения

разрешения доступа к информации и приложениям и получения пароля требуется разрешение тех или иных начальников.

5. Защита файлов - помимо идентификации пользователей и процедур авторизации необходимо разработать процедуры по ограничению доступа к файлам с данными:

а) использовать внешние и внутренние метки файлов для указания типа информации, который они содержат, и требуемого уровня безопасности;

б) ограничить доступ в помещения, в которых хранятся файлы данных (библиотеки данных, архивы);

в) использовать организационные меры и программно-аппаратные средства для ограничения доступа к файлам только авторизованных пользователей; для этого необходимо:

- отключать неиспользуемые терминалы;
- закрывать комнаты, где хранятся терминалы;
- разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются;
- установить специальное оборудование, например, устройства, ограничивающие число неудачных попыток доступа, устройства, обеспечивающие обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру;
- программировать терминал отключаться после определенного периода неиспользования.

6. Защита целостности информации. Вводимая информация должна быть авторизована, полна, точна и должна подвергаться проверкам на ошибки. Необходимо проверять точность информации с помощью процедур сравнения результатов обработки с предполагаемыми результатами обработки. Например, можно сравнивать суммы или проверять последовательные номера.

Нужно проверять точность вводимых данных, проверяя их корректность, например:

а) проверки на нахождение символов в допустимом диапазоне символов (числовом и буквенном);

б) проверки на нахождение числовых данных в допустимом диапазоне чисел;

в) проверки на корректность связей с другими данными, сравнивающими входные данные с данными в других файлах;

г) проверки на разумность, сравнивающие входные данные с ожидаемыми стандартными значениями;

д) ограничения на транзакции, сравнивающие входные данные с административно установленными ограничениями на конкретные транзакции.

7. Защита системных программ. Если программное обеспечение используется совместно, необходимо защищать его от скрытой модификации. Меры защиты при разработке программ должны включать процедуры внесения изменений в программу, ее приемки и тестирования до ввода в эксплуатацию.

8. Адекватные меры защиты. Сделать меры защиты более адекватными можно при помощи привлечения организаций, занимающихся тестированием компьютерной и информационной безопасности, при разработке мер защиты в прикладных программах и консультаций с ними при определении необходимости тестов и проверок при обработке критических данных. Контрольные журналы,

встроенные в компьютерные программы, могут предотвратить или выявить компьютерное мошенничество и злоупотребление.

Должны иметься контрольные журналы для наблюдения за тем, кто из пользователей обновлял критические информационные файлы.

Если критичность информации, хранимой в компьютерах, требует контрольных журналов, то важны как меры физической защиты, так и меры по управлению доступом. В компьютерной сети журналы должны храниться на хвосте, а не на рабочей станции. Контрольные журналы не должны отключаться для повышения скорости работы. Распечатки контрольных журналов должны просматриваться достаточно часто и регулярно.

4.6 Коммуникационная безопасность

Нельзя забывать о том, что данные, передаваемые по незащищенным линиям, могут быть перехвачены.

Электронная почта или e-mail - самый популярный вид использования Интернета. С помощью электронной почты можно послать письмо миллионам людей по всей планете. Электронная почта становится все более важным условием ведения повседневной деятельности, поэтому в организации должна быть разработана политика правильного использования электронной почты, чтобы помочь сотрудникам уменьшить риск умышленного или неумышленного неправильного ее использования и гарантировать, что официальные документы, передаваемые с помощью электронной почты, правильно обрабатываются.

Основные протоколы передачи почты обычно не осуществляют надежной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем. Хотя существуют расширения этих протоколов, решение использовать их должно быть принято как составная часть политики администрации почтового сервера. Некоторые такие расширения используют уже имеющиеся средства аутентификации, а другие позволяют клиенту и серверу согласовать тип аутентификации, который будет использоваться в данном соединении.

Основные угрозы, связанные с использованием электронной почты, представлены в таблице 4.3.

Можно защитить электронную почту с помощью использования шифрования и присоединения к письмам электронных подписей. Одним из популярных методов является использованием шифрования с открытыми ключами.

Важным средством защиты является корректное использование электронной почты. Все служащие должны использовать электронную почту так же, как и любое другое официальное средство организации. Из этого следует, что когда письмо посылается, как отправитель, так и получатель должны гарантировать, что взаимодействие между ними осуществляется согласно принятым правилам взаимодействия. Взаимодействие с помощью почты не должно быть неэтичным, не должно восприниматься как конфликтная ситуация или содержать конфиденциальную информацию.

Таблица 4.3 - Основные угрозы, связанные с использованием электронной почты

Фальшивые адреса отправителя	Адресу отправителя в электронной почте нельзя доверять, так как отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма.
Перехват письма	Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе его передачи по Интернету. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя, или для того, чтобы перенаправить сообщение.
Почтовые бомбы	Это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока не выйдет из строя. Как это может случиться, зависит от типа почтового сервера и того, как он сконфигурирован.
Угрожающие письма	Много почтовых систем имеют возможности фильтрации почты, то есть поиска указанных слов или словосочетаний в заголовке письма или его теле, и последующего помещения его в определенный почтовый ящик или удаления.

4.7 Возможности нападения на компьютерные системы финансового учреждения (банка) и способы отражения этих атак

К нынешним автоматизированным банковским системам (АБС) предъявляются очень строгие требования, как со стороны банков-пользователей, так и со стороны государственных и контролирующих органов. Производители АБС должны динамически подстраивать свою продукцию под изменяющиеся нормативы и отчетные требования, предъявляемые к ведению банковского бизнеса.

Почти все бизнес-процессы финансового учреждения связаны с обработкой или пересылкой некоторой информации. Сейчас вряд ли найдется банк, не автоматизировавший процесс работы с бизнес-информацией. Постоянно растет число банков, использующих Интернет и удаленный доступ к своим системам.

Только комплексная информационная банковская система, интегрирующая различные сферы деятельности банка, способна полностью автоматизировать и объединять в единой целое бизнес-процессы финансового учреждения. Работа с клиентами, начисление процентов, предоставление всевозможных банковских услуг должны быть увязаны с внутрихозяйственной деятельностью банка, с бухгалтерией. Комплексная система, поддерживающая централизованную обработку, мультивалютность и автоматизацию основных финансовых операций, позволяет эффективно проводить управление, контроль, получение отчетов о текущей деятельности всех филиалов банка.

Компьютерная система банка, или АБС, выполняют следующие функции:

- операционный день;
- операции на фондовом рынке;
- работа с ценными бумагами;
- внутрихозяйственная деятельность;
- розничные банковские услуги;
- электронные банковские услуги;
- расчетный центр и платежная система (карточки);
- управление деятельностью банка,
- налоговый учет и отчетность;

- программы лояльности клиентов;
- маркетинговая, рекламная службы.

В компьютерной системе банка содержаться следующие технологии:

- системы управления базами данных;
- хранилища данных;
- информационное, техническое, программное обеспечение;
- антивирусная защита;
- поддержка различных каналов доступа;
- программы реализации банковских операций и другое.

Среди первоочередных эксплуатационных требований, предъявляемых АБС, в первую очередь хотелось бы выделить надежность и безопасность. Сбой программного обеспечения или злоумышленное вторжение в территориально-распределительную банковскую информационную систему могут иметь очень печальные последствия, характеризуемые количественно (величиной ущерба) и качественно (падением имиджа, срывом переговоров и т.п.).

Многочисленные попытки взломов и успешные нападения на банковские вычислительные структуры, и порталы остро ставят проблему обеспечения компьютерной безопасности.

Среди компонентов, образующих АБС выделим следующие, реализуемые путем использования общедоступных сетей:

- банк - клиент;
- интернет - клиент;
- офис - удаленный менеджер;
- головной офис - региональные офисы (отделения);
- интернет – трейдинг.

В таких общедоступных сетях распространены нападения хакеров, которые выводят из строя серверы или проникают в систему безопасности АБС.

Интернет позволяет передавать конфиденциальную информацию практически в любую точку мира, но передаваемые данные необходимо защищать как в плане конфиденциальности, так и в плане обеспечения подлинности, иначе они могут быть искажены и перехвачены. Интернет-систему необходимо защищать от подлога, несанкционированного разрушения, изменения, блокирования работы и т.д.

Комплекс технических средств защиты интернет-сервисов:

1) брандмауэр (межсетевой экран) - программно-аппаратная реализация;
2) системы обнаружения атак на сетевом уровне;
3) антивирусные средства;
4) защита на уровне приложений: протоколы безопасности, шифрования, цифровые сертификаты, системы контроля целостности;
5) защита средствами системы управления базами данных;
6) защита передаваемых по сети компонентов программного обеспечения;
7) мониторинг безопасности и выявление попыток вторжения, адаптивная защита сетей, активный аудит действий пользователей;
8) обманные системы;
9) корректное управление политикой безопасности.

Для обеспечения высокого уровня информационной безопасности компьютерных систем рекомендуется проводить следующие процедуры при организации работы собственного персонала:

- фиксировать в трудовых договорах обязанности персонала по соблюдению конфиденциальности;
- распределять основные функции между сотрудниками, чтобы ни одна операция не могла быть выполнена одним человеком от начала до конца;
- иметь нормативно-правовые документы по вопросам защиты компьютерной информации;
- постоянно повышать квалификацию сотрудников, знакомить их с новейшими методами обеспечения компьютерной безопасности;
- создать базу данных для фиксирования несанкционированного доступа к информации в компьютере;
- проводить служебные расследования в каждом случае нарушения политики безопасности.

Вопросы для повторения темы:

1. Перечислите основные цели компьютерных преступлений.
2. В какие три большие группы объединяют лиц, совершающие компьютерные преступления?
3. Перечислите основные способы компьютерных преступлений в зависимости от способа воздействия на компьютерную систему.
4. Раскройте сущность метода «Логическая бомба». В чем его главное отличие от метода «Временная бомба»?
5. Раскройте сущность уивинга.
6. Назовите метод контроля за компьютерной преступностью.
7. В каких законодательных документах РФ заложены основы регулирования информационных отношений в обществе?
8. Какие мероприятия включает в себя организационное обеспечение компьютерной безопасности?
9. Раскройте принцип работы межсетевого экрана каждого типа.
10. Почему для организации взаимодействия с Internet рекомендуется создание отдельного Internet-сегмента?
11. Что включают в себя программно-технические меры компьютерной безопасности?
12. Что может использоваться в качестве персональных идентификаторов в различных программно-аппаратных средствах защиты?
13. В чем принципиальное различие симметричного и ассиметричного метода шифрования?
14. Перечислите основные признаки, свидетельствующие о наличии уязвимых мест в компьютерной безопасности.
15. Какие меры должен принимать пользователь компьютера с целью защиты информации?
16. Что является объект Ом коммуникационной безопасности?
17. Перечислите основные угрозы, связанные с использованием электронной почты?

18. Что включает в себя комплекс технических средств защиты интернет-сервисов?

Литература:

1. Карабаналов С. С. Компьютерные мошенничества // Финансовый бизнес. - 2002. - ноябрь - декабрь

2. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. - М.: Горячая линия-Телеком, 2002. - 336 с.

3. Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы / Борис Леонтьев. - 3-е изд., - М.: Майор, 2002. - 192 с. - (Серия книг «Мой компьютер»)

4. Макклуре С, Скембрэй Дж., Куртц Дж. Секреты хакеров. Проблемы и решения сетевой защиты. - М.: Издательство «ЛОРИ», 2001. - 434 с.

5. Мельников Ю., Теренин А. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак // Банковские технологии. - 2003. - № 1

6. Мельников Ю., Теренин А. Возможности нападения на информационные системы банка из Интернета и некоторые способы отражения этих атак (окончание) // Банковские технологии. - 2003. - № 2

7. Петровский А. И. Эффективный хакинг для начинающих и не только / Алексей Петровский. - 3-е изд., - М.: Майор, 2002. - 192 с. - (Серия книг «Мой компьютер»).

8. Ярочкин В. И. Безопасность информационных систем. - М., 1996

Глава 5. Слияния и поглощения. Методы защиты

Ключевые понятия:

«Враждебное поглощение»
Симбиозом
Сохранение статуса
Адсорбция
Разделенный совет
Супербольшинство
Справедливая цена
"Ядовитая пилюля"
Рекапитализация высшего класса
Защита Пэкмена
Реструктуризация активов
Preferred stock plans;
Flip-over plans;
Flip-in plans;
Flip-out plans;
Back-end plans;
Voting plans).
Компенсационные парашюты
Реинкорпорация

5.1 Общие положения

В рыночной экономике одним из цивилизованных инструментов перераспределения собственности являются сделки на рынке корпоративного контроля – слияния и поглощения. Принцип лежащий в основе этого рынка, заключается в прямой зависимости рыночной стоимости акций компании от эффективности её управления. В России рынок корпоративного контроля пока не получил такого большого развития, как на западе, однако развивается стремительными темпами. С учётом национальной специфики именно враждебное поглощение становится в нашей стране доминирующей формой всех поглощений.

Само понятие «**враждебное поглощение**» пришло в Россию из США. Как перевод английского термина HOS-TILE TAKE-OVER (скупка группой лиц или лицом контрольного пакета акций без согласия его руководителей).В нашей стране этот термин вытеснен другим более распространённым в народе понятием – «передел собственности».

Первый опыт враждебных поглощений относят к середине 90-х годов. Один из первых примеров публичной операции поглощения стала попытка захвата кондитерской фабрики «Красный октябрь» группой банков Менатеп. Летом 1995 г. В России при осуществлении враждебного поглощения широко используются различные методы давления на менеджмент «компании-жертвы» как силовые, так и административные, а также лоббирование необходимых решений.

Стратегия слияния или поглощения вырабатывается на основе общей стратегии развития компании. На самом высшем уровне оценивается, насколько рассматриваемое слияние или поглощение соответствует миссии и целям предприятия, насколько вписывается в общую стратегию и как органично может войти в план мероприятий по реализации стратегии. В наиболее общем виде процесс принятия решений о слияниях и поглощениях можно рассмотреть, исходя из сопоставления типовых разделов стратегического плана фирмы с возможностью слияния или поглощения (Таблица 5.1).

Процесс слияний и поглощений состоит из шести этапов. Первые три этапа представляют собой процесс планирования слияния и поглощения, проведение аналитической работы по потенциальному объекту слияния или поглощения, переговоры о возможном слиянии или соглашении, подготовку и подписание соответствующего соглашения. Вторые три этапа - практическая реализация проекта. Основные этапы сделки по слиянию или поглощению:

1. Разработка стратегии слияний и поглощений;
2. Анализ потенциального объекта слияния или поглощения;
3. Переговорный процесс и заключение соглашения;
4. Оценка и стабилизация положения;
5. Интеграция;
6. Постинтеграция.

Разработка стратегии слияния или поглощения является отражением общей стратегии компании, что подразумевает оценку её положения на рынке, анализ сильных и слабых сторон, рассмотрение возможностей и угроз для развития бизнеса, анализ конкурентов. Стандартные параметры анализа конкурентов включают оценку стратегии, продуктового ряда, клиентской базы и рынков.

По результатам формирования общеё стратегии компании формируются цели слияния или поглощения: кто нужен для осуществления приоритетных задач. Если предполагается выход на новые рынки, то должны учитываться:

- соотношение риска и доходности;
- цели развития бизнеса, основные области, в которых ведется и будет вестись бизнес, специализация и имидж организации;
- требования к величине собственного капитала и к показателям достаточности капитала (при выходе на международные рынки следует учитывать и требования регулирующих органов стран, где предполагается вести бизнес);

Таблица 5.1 – Сопоставление стратегического плана фирмы с возможностью слияния или поглощения

Типовое содержание стратегического плана	Вопрос слияния или поглощения
Миссия (главная цель существования организации)	Насколько предлагаемое слияние или поглощение отвечает миссии организации?
Цели (финансовые, размер бизнеса, эффективность операций)	Каким образом предлагаемое слияние или поглощение будет способствовать осуществлению целей организации?
Макроэкономические тенденции и предпосылки развития рынка	Насколько макроэкономические тенденции (включая государственное регулирование), возможности рынка будут адекватны для проведения слияния или поглощения?
Оценка конкурентоспособности организации	Насколько слияние или поглощение повысит конкурентоспособность организации? Как укрепятся сильные стороны, удастся ли решить проблемные аспекты?
Оценка возможностей развития	Каким образом слияние или поглощение будет способствовать оптимальному использованию возможностей развития? Удастся ли нивелировать угрозы?
Стратегии по основным сегментам рынка	Какое воздействие слияния или поглощения на позицию компании во всех сегментах рынка окажет слияние или поглощение?
Стратегические задачи по основным видам деятельности	Будут ли достигнуты необходимые результаты по основным видам деятельности?
Планы мероприятий по реализации основных стратегических задач	Насколько слияние или поглощение будет способствовать реализации планов мероприятий?
Ожидаемые финансовые результаты	Насколько слияние или поглощение будет способствовать достижению установленных показателей?

- законодательная и нормативная база;
- конкуренция на национальном и международных рынках;
- макроэкономические параметры и условия;
- маркетинговое исследование наиболее важных для бизнеса клиентских групп.

Стратегический уровень предполагает выбор объекта для слияния или поглощения, которому предшествует тщательный и многовариантный анализ реализации стратегии развития. Компания-покупатель проводит оценку своих стратегических намерений и определяет оптимальный связи с бизнесом присоединяемой компании, после чего выбирается стратегия присоединения.

Стратегические намерения можно разделить на:

- симбиоз;
- адсорбцию;
- сохранение статуса.

Под **симбиозом** понимается взаимопроникновение двух структур: это может быть обмен крупными пакетами акций, ведущий к объединению ряда операций на финансовых рынках, взаимодополнение продуктового ряда и т.п. Здесь типичным примером может послужить договор об объединении Юкоса и Сибнефти.

Адсорбция есть полное слияние или поглощение (это означает, что из двух вступивших в сделку структур на рынке остается только одна). В качестве примера адсорбции можно привести слияние Bank of America и Nations Bank.

При поглощении возможно **сохранение статуса** (имеется в виду формальный статус организации; например, одной из стратегий развития National Australia Bank является поглощение региональных банков в разных регионах мира при сохранении их формального статуса - в Великобритании собственностью National Australia Bank являются Clydesdale Bank, Yorkshire Bank и Northern Bank).

Используемая стратегия может быть:

- агрессивной,
- защитной,
- наблюдательной.

На основе выявленных характеристик компании - объекта поглощения результаты проведенного анализа сопоставляют со стратегическими целями покупателя на предмет соответствия этим целям. Сопоставление проводится как на уровне миссии и целей, так и на уровне плана мероприятий по реализации стратегии.

5.2 Прикладные аспекты слияний и поглощений: международная практика и российские особенности.

Известно, что выбор объекта слияния или поглощения представляет собой очень непростую задачу и осуществляется на основе стратегии развития. Определение объекта слияния или поглощения включает как сбор и обработку информации. Мы рассмотрим основные подходы практиков и технологии, применяемые для выбора цели поглощения.

После того, как общая стратегия слияния или поглощения сформулирована в рамках определения четких критериев, приступают к поиску подходящего объекта слияния или поглощения.

В практике подобный поиск заключается в работе с различными базами данных, в том числе в Интернет. Возможно, что будет обработан большой объем статистических данных и аналитической информации.

1. Публикуемые годовые отчеты.

Один из важных аспектов - как быстро появляется годовой отчет по окончании финансового года (нормальным представляется срок не более четырех месяцев после окончания финансового года, хорошим - не более трех месяцев). Если годовой отчет публикуется значительно позже, то это может означать: наличие невысокого уровня аппаратной работы, недостаточно высокий уровень бухгалтерского учета и отчетности (значительное время, ушедшее на проведение годового аудита). Не исключаются попытки сокрытия информации. Как правило, годовые отчеты публикуются в периодических изданиях, на Интернет-сайтах компании.

2. Информация о предоставляемых компанией услугах (рекламные материалы, другая информация для клиентов).

На основе рекламных материалов и информации для клиентов формируется перечень услуг и товаров, оказываемых или выпускаемых предприятием. Оценка

качества и полноты рекламных и информационных материалов даст возможность понять уровень и качество работы маркетингового подразделения.

3. История фирмы.

Знания истории компании оказывается весьма полезными для понимания корпоративной культуры, сложившейся организационной структуры, характера управления, внутренних процедур и систем контроля. История может быть полезна для понимания соотношения сил между различными группами участников и высшего руководства, возможен прогноз преемственности высшего руководства.

4. Реклама.

Развертывание рекламной компании обосновывается той или иной балансово-структурной политикой, вызывается необходимостью продвижения новых продуктов на рынке. Интересно оценить, насколько адекватен и своевременен выбор того или иного средства массовой информации для достижения максимального эффекта рекламной кампании.

5. Средства массовой информации.

Информация о компании, получаемая из газет, журналов (как общего характера, так и специальных) является наиболее доступной, хотя далеко не всегда объективной (в настоящее время в России очень часто появляются "заказные" статьи, причем заказчиком может быть как само предприятие, так и конкуренты). Активное использование поисковых систем сети Интернет существенно упрощает сбор и обработку информации из упомянутого источника и облегчает необходимую аналитическую работу.

6. Сайт в сети Интернет.

Само по себе наличие сайта компании в Интернете говорит о его стремлении к развитию информационных технологий, о стремлении к определенной открытости. Полезна общая оценка качества сайта, дизайн (включая информацию о разработчике), удобство для потребителя, своевременность и точность представленной информации, наличие возможности получения новостей об организации путем подписки (безусловно, возможность подписки следует использовать). Важно понять, предоставляет ли компания услуги через Интернет, если да, то каково качество этих услуг, характер системы защиты информации. Есть одно немаловажное наблюдение: в периоды значительных финансовых затруднений организации ослабляют контроль за своевременностью и точностью информации, размещаемой ими в сети Интернет.

7. Выступления высших должностных лиц компании.

Выступления высших должностных лиц компании полезны, прежде всего, для оценки стратегии, общественной деятельности, не исключено, что анализ выступлений руководителей даст оценку качества работы сотрудников аппарата, в некоторых случаях возможно получить информацию о тех или иных проблемах фирмы. Указанные выступления могут содержать сведения о переменах в организационной структуре, кадровой политике и т.п.

8. Информация, получаемая от клиентов компании.

В первую очередь, наибольший интерес представляет информация о качестве предоставляемых услуг, о работе персонала с клиентурой. Возможно, что удастся получить информацию о внутренних процедурах компании.

9. Поставщики.

Информация о поставщиках позволяет дать косвенную оценку перспективным направлениям развития. Эта информация необходима и для оценки текущих и потенциальных затрат, понимания качества и уровня хозяйственного управления фирмой.

10. Консультанты организации.

Многие компании время от времени привлекают внештатных консультантов. Прежде всего, консультантов используют при решении проблем маркетинга, в процессе стратегического планирования, при разработке систем управленческой информации, для формирования кадровой политики, включая подбор персонала. Сильные и слабые стороны консультантов и консалтинговых фирм, их специализация, известны на рынке, поэтому, зная, каких консультантов привлекла компания, можно с весьма высокой степенью вероятности определить пути его развития по тому направлению, на котором работают консультанты.

11. Анализ качества услуг или продукции компании.

Анализ качества продукции (услуг) компании может проводиться как самостоятельно, так и путем привлечения специализированных фирм. Очень важно объективно показать как негативные, так и позитивные аспекты.

12. Сведения о нанятом компанией персонале.

Приоритетной является информация о ключевых специалистах по организационной структуре фирмы. Переход сотрудников можно использовать для получения информации. Может оказаться эффективным устанавливать системы поиска в Интернете по интересующим персоналиям (можно проследить назначения и перемещения, публикации).

13. Сведения, получаемые от бывших руководящих сотрудников фирмы, нанятых в качестве консультантов.

Бывает полезно для получения информации об организации принимать на работу в качестве консультантов бывших руководящих сотрудников компании. Подобные консультанты могут стать источником чрезвычайно полезной информации о корпоративной культуре, внутреннем контроле и регулировании, системах управленческой информации, стратегии. Возможно использование данной категории для работы по клиентуре и персоналу конкурента.

14. Сведения, получаемые иными путями.

Существуют и иные, незаконные способы получения информации: подкуп чиновников местной администрации, подкуп сотрудников, держателя реестра и т.д.

После сбора информации составляется досье по объекту слияния или поглощения, которое для "короткого списка" может выглядеть следующим образом:

1. Название организации.
2. Сведения о владельцах (основных акционерах).
3. Количество и месторасположение головной конторы, филиалов, отделений, дочерних и родственных структур.
4. Количество и должностная структура персонала (в разрезе структурных подразделений, по направлениям деятельности, по территориальному расположению).
5. Организационная структура (желательно иметь максимально детализированную организационную структуру).

6. Информация о финансовых результатах как компании в целом, так и его филиалов, отделений, дочерних и родственных структур.

7. Информация об услугах (диапазон оказываемых услуг, качество и стоимость оказываемых услуг).

8. Информация о доле компании на рынке (сегментация по типам клиентов, по продуктам, по регионам).

9. Информация о рекламе (оценка расходов, качества, целевой направленности рекламы, рекламируемые услуги, используемые способы рекламы, задействованные средства массовой информации).

10.Сайт в сети Интернет (адрес, структура, содержательная часть, периодичность обновления, качество).

11.Информация по основной клиентуре и сегментам рынка (в различных аспектах).

12.Информация о специфических продуктах (услугах) и сегментах рынка (если таковые имеются).

13.Информация об исследовательской деятельности и разработках (основные направления исследований, наиболее важные проекты, информация о задействованном в работе персонале).

14.Информация об основных поставщиках (наименование, вид поставляемых изделий и услуг, стоимость изделий и услуг, информация о заключенных договорах).

15.Информация о качестве персонала, зарплате, технологии работы с персоналом, системе повышения квалификации.

16.Сведения о ключевых фигурах на фирме (личные данные, профессиональный опыт, занимаемая должность, уровень оплаты).

17.Информация о персоналиях, входящих в наблюдательный совет и ревизионную комиссию.

18.Сведения о системах контроля (включая безопасность), планирования, управленческой информации (в том числе типовые формы отчетности и управленческой информации).

На этой стадии подготовки сделки (работа по "короткому списку") команда должна выработать полное понимание особенностей того или иного вида бизнеса и точно представлять себе факторы, оказывающие позитивное или негативное влияние, как на избранные объекты поглощения, так и на рынок в целом. Необходимую информацию по рынкам, на которых оперирует деловое предприятие, можно получить из отчетов и информационных бюллетеней, публикуемых правительством, консалтинговыми и аудиторскими фирмами, отраслевыми ассоциациями: это информация о размере рынка, перспективах роста, чувствительности отрасли к макроэкономическим тенденциям, сведения об основных участниках рынка, иностранных конкурентах, а также о проблемах государственного регулирования, законодательства, экологических аспектах.

Специалистами консалтинговой компании Accenture была разработана модель определения цели поглощения по ряду параметров. Выделяются пять ключевых категорий для слияний и поглощений (Рисунок 5.1).

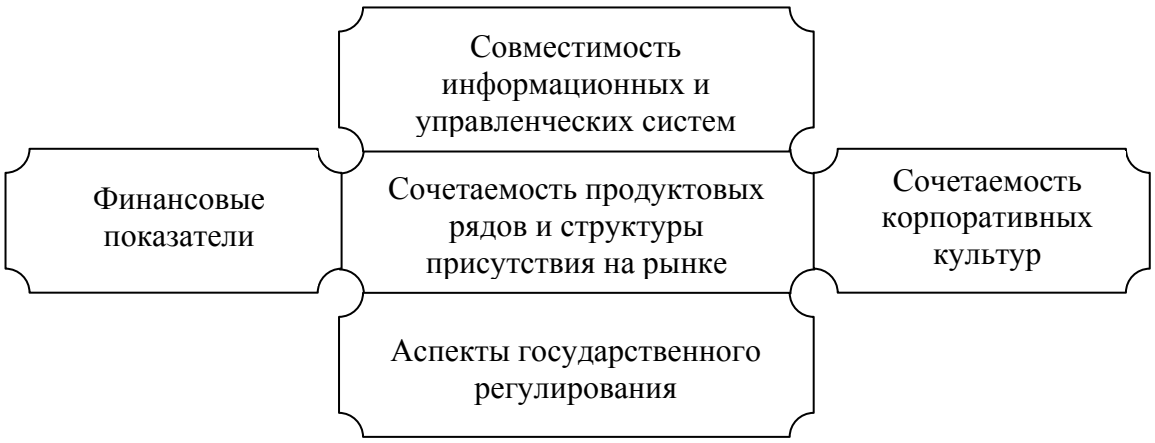

Рисунок 5.1 – Категории слияний и поглощений

Например, категория "финансовые показатели" включает два основных фактора: оценка прироста активов и показатель прибыли до налогообложения в расчете на одного работника. Для первого фактора устанавливается разница между активами поглощающей и поглощаемой стороны и определяется цель, которую нужно достичь поглощающей стороне для выполнения своих стратегических задач. Что касается второго фактора, то проводится анализ на предмет того, повысит ли поглощение эффективность организации. Один из четырех факторов в разделе "сочетаемость корпоративных культур" - стиль руководства. Здесь проводится анализ стиля руководства поглощаемой организации (например, демократичный или авторитарный) и делается сравнение со стилем руководства поглощающей организации.

В целом, проводится анализ и ранжирование каждого фактора для всех пяти категорий и рассчитывается общий балл для каждой категории. Общие баллы по категориям "взвешиваются" для того, чтобы более точно отразить ценность новой организации по критериям рынка: финансовые показатели и сочетаемость продуктовых рядов и структуры присутствия на рынке получают по 25% от общего итога, сочетаемость корпоративных культур и совместимость информационных и управленческих систем - по 20% каждый, аспекты государственного регулирования - 10%. В дальнейшем проводится сопоставление целей поглощения из "короткого списка" по совокупности параметров. Также необходимо подчеркнуть, что никакая модель не является идеальной, поэтому оптимальный результат получается при разумном сочетании подходов.

5.3 Защита от "недружественного поглощения": теория и практика

Защита от "недружественного поглощения" - это действия менеджмента и/или владельцев цели поглощения, направленные на предотвращение попыток ее приобретения или установления определенной степени контроля. Развитие процесса слияний и поглощений в мировом бизнесе в условиях разнообразных и подчас противоположных деловых интересов разных групп владельцев и менеджеров компаний стало основой для формирования различных способов защиты от недружественного поглощения.

За многолетнюю практику на финансовых рынках были выработаны определенные технологии защиты от "недружественного поглощения". В таблице 5.2 кратко описываются основные виды защиты.

Таблица 5.2 - Краткое описание видов защиты от "недружественного поглощения"

Тип защиты	Описание
"Противоакульи поправки к уставу"	
Разделенный совет	Совет делится на три равные группы. Каждый год избирается только одна группа. Поэтому захватчик не может получить контроль над мишенью сразу же после получения большинства голосов.
Супербольшинство	Высокий процент акций, необходимый для одобрения слияния, обычно 80%.
Справедливая цена	Ограничивает слияния акционерам, владеющим более чем определенной долей акций в обращении, если не платится справедливая цена (определяемая формулой или процедурой оценки).
Прочие	
"Ядовитая пилюля"	Для существующих акционеров выпускаются права, которые в случае покупки значительной доли акций захватчиком могут быть использованы для приобретения обыкновенных акций компании по низкой цене, обычно до половины рыночной цены. В случае слияния права могут быть использованы для приобретения акций покупающей компании.
Рекапитализация высшего класса	Распространение обыкновенных акций нового класса с более высокими правами голоса. Позволяет менеджерам компании-мишени получить большинство голосов без владения большей долей акций.
Защита после предложения	
Защита Пэкмена	Контр нападение на акции захватчика.
Тяжба	Возбуждается судебное разбирательство против захватчика за нарушение антитрестовского закона или закона о ценных бумагах.
Реструктуризация активов	Покупка активов, которые не понравятся захватчику или которые создадут антитрестовские проблемы.
Реструктуризация обязательств (пассивов)	Выпуск акций для дружественной третьей стороны или увеличение числа акционеров. Выкуп акций с премией у существующих акционеров.

Как следует из вышеприведенной таблицы, методы защиты весьма разнообразны. Все меры, которые может использовать цель поглощения, можно разделить на "защиту до предложения" и "защиту после предложения". К числу методов "защиты до предложения" относятся разделение совета директоров, супербольшинство, справедливая цена, ядовитые пилюли и рекапитализация высшего класса. К числу методов "защиты после предложения" относятся целевой выкуп, стоп-соглашение, тяжба, реструктуризация активов и реструктуризация пассивов.

Рассмотрим способы защиты от "недружественного поглощения" более подробно.

Разделение совета директоров означает, что в устав корпорации - цели поглощения вносится пункт, в котором оговаривается порядок разделения совета директоров на три равные части; при этом каждая часть совета директоров может быть избрана общим собранием акционеров на один год и так в течение трех лет. Таким образом, ограничиваются возможности "агрессора" получить немедленный контроль над компанией - целью поглощения непосредственно после покупки контрольного пакета акций: компания-покупатель будет вынуждена ждать еще два года для того, чтобы получить необходимое большинство в совете директоров. На практике же подобное ограничение в большом числе случаев снимается, если "агрессор" имеет реальные шансы получить контроль над целью поглощения. Тем

не менее, более половины компаний, входящих в индекс Standard&Poor's 500, использует такой способ защиты, так как это реально усложняет и удорожает поглощение.

Условие супербольшинства есть способ защиты, при котором происходит внесение в устав корпорации - цели оговорки, предусматривающей установление высокого процента голосов, необходимого для принятия решения о слиянии. Во многих случаях это ограничение одновременно распространяют и на такие операции, как принятие решений о ликвидации компании, ее перестройке, продаже или финансовом лизинге крупных активов, принадлежащих компании и т.п. Большинство корпораций, применяющих этот метод защиты, устанавливает количественный барьер голосов для принятия решения о слиянии на уровне от 2/3 до 80%. Условия супербольшинства автоматически применяются ко всем сделкам, в которых участвуют заинтересованные стороны или крупные акционеры. В дополнение, условие супербольшинства сопровождается оговоркой, которая распространяет данное условие на голосование по снятию защиты с корпорации. Естественно, что подобное ограничение значительно ограничивает возможности недружественного поглощения: для обеспечения контроля "агрессору" требуются значительно большие ресурсы.

Условие справедливой цены - внесение в устав корпорации-цели оговорки, определяющей условия выкупа более 20% (возможно, более 30%) голосующих акций. Реально условие справедливой цены является ужесточением условия супербольшинства и, как правило, не применяется отдельно от него. Справедливая цена определяется как одинаковая цена выкупа для любой акции корпорации-цели. Основная цель этого метода защиты - предотвращение двухстадийных тендерных предложений корпорацией-покупателем. Двухстадийное (two-tier) предложение означает, что сначала делается предложение на покупку только крупных пакетов акций (более 5%), затем предлагается купить мелкие пакеты, но по более низкой цене. Естественно, что такая схема ущемляет интересы миноритарных акционеров. Кроме того, существует возможность купить корпорацию по цене ниже рыночной. Большинство корпораций, применявших этот метод защиты, устанавливали "справедливую цену" на основе исторической стоимости своих акций за последние 3-5 лет. Если корпорация-покупатель выполняет условие справедливой цены, в большинстве случаев снимается условие супербольшинства. Защита "справедливой ценой" может быть снята в следующих случаях:

- если снятие защиты будет одобрено 95% акционеров корпорации-цели;
- при дружественном слиянии.

"**Ядовитые пилюли**" в самом общем виде представляют собой эмитированные корпорацией-целью права, размещенные между ее акционерами и дающие им право на выкуп дополнительного количества обыкновенных акций компании при наступлении определенного события. Катализатором исполнения права выкупа может стать любая попытка изменения контроля над данной корпорацией, не согласованная с советом директоров. Ниже мы рассматрим основные виды "ядовитых пилюль":

1. Preferred stock plans;
2. Flip-over plans;
3. Flip-in plans;

4. Flip-out plans;
5. Back-end plans;
6. Voting plans).

Preferred stock plan по существу представляет собой эмиссию корпорацией-целью конвертируемых привилегированных акций, которые распределяются между акционерами в качестве дивидендов. Эти привилегированные акции приравниваются по праву голоса к обыкновенным акциям. Выпуск подобных привилегированных акций приводит к снижению дивидендов по обыкновенным акциям, кроме того, размер дивидендов по привилегированным акциям устанавливается на значительно более высоком уровне, чем по обыкновенным акциям: здесь преследуется цель того, чтобы владельцы привилегированных акций воздерживались от их конвертации в обыкновенные. Эмитент оставляет за собой право выкупа привилегированных акций через определенный период (на практике - не менее 15 лет).

Принцип защиты реализуется следующим образом. В условиях распределения привилегированных акций содержится пункт, в котором оговаривается, что в случае покупки иным инвестором "значительного" пакета обыкновенных акций владельцы привилегированных акций имеют право потребовать от своей компании выкупа этих привилегированных акций, если владелец "значительного" пакета акций в течение небольшого времени не объявит решение о дружественном слиянии с эмитентом. После получения требования о выкупе корпорация должна выкупить привилегированные акции по цене, не ниже:

а) максимальной цены, уплаченной владельцем "значительного" пакета за привилегированные акции, приобретенные им в течение предыдущего года,

б) максимальной цены, уплаченной владельцем "значительного" пакета акций за обыкновенные акции, приобретенные им в течение предыдущего года, умноженной на коэффициент конвертации.

Если же решение о поглощении принимается, то владельцы привилегированных акций лишаются права их выкупа своей компанией. В результате привилегированные акции должны будут конвертироваться в обыкновенные акции поглотившей компании.

Flip-over plan представляют собой следующее. Корпорация-цель объявляет о выплате дивидендов по обыкновенным акциям в форме прав на покупку определенного класса своих ценных бумаг, как правило, обыкновенных акций. Цена исполнения права устанавливается на уровне, значительно превышающем рыночную стоимость ценных бумаг, на покупку которых предоставлено данное право. В дополнение, эти права не могут быть реализованы до наступления определенного эмиссионного события. Таким событием может быть приобретение корпорацией-покупателем значительного пакета голосующих акций или получение предложения на приобретение такого пакета. После наступления подобного события акционеры корпорации-цели не могут осуществить свои права в течение короткого промежутка времени (как правило, 10 дней). По истечении указанного времени права могут быть реализованы, и корпорация-цель распределяет сертификаты этих прав. До этого момента обыкновенные акции и права не могут торговаться отдельно друг от друга. Досрочный выкуп возможен, но он проводится со значительным дисконтом. В результате в случае принятия решения о поглощении акционеры

поглощенной компании будут иметь возможность очень выгодно купить акции компании, возникшей после поглощения, что может оказаться очень дорогим для поглощающей стороны.

Flip-in plan по существу есть дополнение к предыдущему способу защиты. Суть его заключается в следующем: если корпорация-покупатель переводит активы купленной корпорации на дискриминирующие ее акционеров условиях или на условиях, снижающих стоимость вложения, то акционеры корпорации-цели имеют право выкупить акции корпорации-покупателя со значительным дисконтом их рыночной стоимости. Таким образом обеспечивается защита акционеров поглощаемой стороны; кроме того, покупка может стать более дорогостоящей для корпорации-покупателя.

Flip-out plan - способ защиты, при котором акционеры компании - цели поглощения получают право на выкуп акций "агрессора", что по существу есть контрнападение на этого "агрессора". Это напоминает защиту Пэкмена, о которой пойдет речь ниже. Разумеется, для реализации подобного способа защиты требуются значительные финансовые ресурсы.

Процедура защиты **Back-end plan** почти полностью повторяет flip-over plans, за исключением того, что распределяются права на покупку долговых инструментов, а не обыкновенных акций. Корпорация-покупатель после проведения поглощения сталкивается с проблемой обслуживания большого объема долговых обязательств (основной долг и проценты). Долг создается с целью защиты компанией - целью поглощения.

Основная задача **Voting plan** в том, чтобы предотвратить попытку получения контроля над корпорацией одного лица либо группы лиц путем простого большинства голосов. Суть метода заключается в том, что корпорация - цель поглощения объявляет своим акционерам о выплате дивидендов в виде привилегированных акций. В случае если отдельное лицо или группа лиц становится владельцем "значительного" пакета обыкновенных и привилегированных акций, владельцы привилегированных акций, за исключением обладателя "значительного" пакета, получают право суперголоса, что не дает возможность получить контроль над компанией владельцу этого "значительного" пакета.

Рекапитализация высшего класса как метод защиты сводится к следующему. Все эмитированные компанией акции делятся на два класса: акции с обыкновенным правом голоса (низший класс акций) и акции с повышенным правом голоса (высший класс акций). Обычно акции низшего класса голосуют по принципу "одна акция - один голос", а акции высшего класса - "одна акция - десять голосов". Акции высшего класса размещаются только среди акционеров компании - цели поглощения. Они могут быть через определенное время обменены на акции низшего класса (обыкновенные акции). Как правило, дивиденды по акциям высшего класса устанавливаются на более низком уровне, чем по акциям низшего класса; кроме того, акции высшего класса всегда низколиквидны, и могут вообще не обращаться на фондовом рынке. Главная цель выпуска акций высшего класса - как можно скорее заставить их владельцев обменять их на акции низшего класса. Также устанавливается, что менеджеры корпораций-аутсайдеров не могут быть участниками подобного обмена (рекапитализации). После проведения подобной

рекапитализации менеджмент корпорации-цели, даже обладая относительно небольшим пакетом обыкновенных акций, будет способен эффективно блокировать попытки изменения контроля над корпорацией. Практика показывает, что данный метод весьма эффективен.

При **целевом выкупе** компания - цель поглощения делает прямое тендерное предложение внешнему инвестору или группе инвесторов, которые уже владеют крупным пакетом ее обыкновенных акций и могут представлять потенциальную угрозу. Выкуп производится со значительной премией по сравнению с рыночным курсом акций. При помощи этого метода ликвидируется потенциальная угроза "недружественного поглощения". Естественно, что успех данного метода защиты в наибольшей степени определяется величиной предлагаемой премии над текущим рыночным курсом.

Соглашение о невмешательстве (стоп-соглашение) представляет собой контракт, который заключается между менеджментом компании - цели поглощения и крупным акционером, согласно которому этот крупный акционер обязуется не владеть контрольным пакетом акций на протяжении определенного времени.

Тяжба - один из самых популярных видов защиты после получения предложения о поглощении. Более 1/3 всех тендерных предложений, сделанных в США за период с 1982 по 2002 год, сопровождались возбуждением различных судебных исков со стороны корпорации-цели. При этом корпорация-покупатель обвинялась в нарушении всевозможных видов законодательства, включая природоохранное. Большинство исков подаются в связи с антимонопольным законодательством и законодательством, регулирующим фондовый рынок.

В результате начала тяжбы корпорация-цель может задержать проведение "недружественного поглощения" (судебные процедуры, слушания, пересмотр дела и т.п.) и одновременно увеличить стоимость поглощения (более интересно увеличить размер тендерного предложения, чем нести значительные судебные издержки). Кроме того, возможна такая технология возбуждения тяжбы, когда иск учиняет "дружественная" поглощаемой компании фирма или частное лицо на основе предварительного сбора информации компанией-целью.

Реструктуризация активов - продажа и покупка активов, которая совершается для того, чтобы сделать объект поглощения менее привлекательным для "агрессора". Возможна продажа привлекательных активов, что снижает инвестиционную привлекательность поглощаемой компании, или покупка такого бизнеса, когда дальнейшая его консолидация за счет "недружественного поглощения" может привести к проблемам с органами государственного регулирования, например, антимонопольными органами.

Реструктуризация пассивов представляет собой следующее:

1. Проведение дополнительной эмиссии обыкновенных акций, полностью размещаемой среди дружественных внешних инвесторов (или акционеров), то есть лиц, которые поддержат существующий менеджмент корпорации-цели в случае попытки "недружественного поглощения".

2. Проведение крупной эмиссии долговых обязательств (краткосрочных или долгосрочных облигаций); одновременно средства, полученные от проведения эмиссии, направляются на выкуп своих обыкновенных акций, обращающихся на рынке или находящихся у крупных, но "неблагонадежных" акционеров.

В первом случае подобная защита обеспечивает больше шансов менеджменту на сохранение статуса при голосовании на общем собрании акционеров.

Во втором случае увеличение внешней задолженности корпорации снижает ее инвестиционную привлекательность; кроме того, дополнительно проводимый выкуп значительно усложняет процесс приобретения контрольного пакета акций компании за счет снижения количества акций, доступных для покупки "агрессором".

После рассмотрения групп методов защиты "до предложения" и "после предложения" представляется целесообразным остановиться на некоторых специфических способах защиты, встречающихся на практике.

Реинкорпорация означает переоформление учредительных документов в другой регион (перенос юридического адреса), где существуют более жесткие антимонопольные требования, чем по текущему месту регистрации. Подобная защита может значительно затруднить поглощение реинкорпорированной компании, но процесс оформления документов может потребовать много времени, что может оказаться совсем не в интересах защищающейся стороны.

Компенсационными парашютами называют включаемые в контракты менеджеров условия, гарантирующие значительные выплаты этим менеджерам в случае "недружественного поглощения" или "не согласованного с менеджерами" поглощения. Естественной практикой поглощающей компании является замена ключевых менеджеров поглощаемой компании.

Компенсационные парашюты бывают:

- золотыми (компенсационные соглашения заключаются с высшим менеджментом);
- серебряными (компенсационные соглашения заключаются с менеджментом среднего звена);
- оловянными (компенсационные соглашения заключаются с менеджментом низшего звена и некоторыми рядовыми сотрудниками компании).

Если компенсационные соглашения составлены юридически безукоризненно, и сумма компенсации существенна, то у поглощающей компании возможны проблемы. Кроме того, наличие подобных контрактов является стимулом для менеджмента компании проводить эффективные защитные действия, если этого требуют акционеры.

Рынок может отреагировать на применение такого способа защиты как позитивно (рост котировок акций на 1,5-3%), так и негативно (падение цены акций на 1% и более). Реакция рынка в большом числе случаев зависит от типа контракта: менеджмент - акционеры или менеджмент - менеджмент. По мнению некоторых исследователей, в среднем такой метод защиты не дает компании ни выигрыша, ни проигрыша.

Как правило, подобные контракты редко превышают 1 год. Обычной практикой считается заключение таких контрактов за 6-8 месяцев до "недружественного поглощения".

Белый рыцарь и белый сквайр - способы защиты, когда для поглощения приглашается дружественный акционерам инвестор. При выборе способа защиты белый рыцарь корпорация-цель пытается помешать "недружественному захвату" путем осуществления дружественного поглощения, продавая свой контрольный пакет акций дружественной менеджменту корпорации. Размер предложения,

которое делает "белый рыцарь", определяется, главным образом, тем, насколько подобная сделка вписывается в его стратегию. Если соответствие стратегии - хорошее, то цена может быть выше предложенной "агрессором", если же уровень соответствия стратегии невелик, то цена будет ниже. На практике же возможна ситуация, когда "агрессор" будет повышать цену, не отказываясь от попытки "недружественного захвата" даже после появления "белого рыцаря": тогда цена будет расти.

Защита белый сквайр отличается от защиты "белый рыцарь" тем, что белый сквайр не получает контроля над целью поглощения. Дружественная к менеджменту компания - белый сквайр покупает по предложению цели поглощения крупный пакет акций на "условиях невмешательства" (обычно это означает обязательство голосовать за предложения менеджмента). Таким образом, "агрессор" лишается возможности получить большинство голосов на собрании акционеров и, следовательно, решить проблему поглощения. В качестве вознаграждения белый сквайр обычно получает места в совете директоров или повышенные дивиденды на купленные акции.

Защита Пэкмена (PacMan defense) заключается в контрнападении корпорации - цели поглощения на корпорацию - агрессора в случае попытки жесткого поглощения (корпорация-цель делает встречное тендерное предложение акционерам корпорации-покупателя на выкуп контрольного пакета ее акций). Подобная практика встречается очень редко, так как основная проблема с ее применением - значительный объем финансовых ресурсов, необходимых для проведения контрнаступления на покупателя. Поэтому только корпорация-цель, которая значительно превосходит корпорацию-поглотителя свободными финансовыми ресурсами, может рассчитывать на успешное проведение такой защиты.

5.4 Рекомендации по защите от поглощений в России

Практика "недружественных поглощений" российских промышленных и торговых компаний достаточно обширна. Рассмотрим рекомендации, которые российские практики дают в части противостояния недружественному поглощению:

1. Защита реестра акционеров от несанкционированного доступа. Человек со стороны не знает, у кого находятся акции. Без доступа к реестру произвести скупку акций за короткий срок крайне сложно. Таким образом, опасно держать реестр у мелких реестродержателей.
2. Лучше всего с самого начала написать защищающий от поглощений устав.
3. Заключение трудовых договоров с руководством компании, в которых оговариваются значительные компенсации в случае увольнения.
4. Консолидация разобщенного пакета. Скупка акций у физических лиц (мелких держателей) с целью увеличения пакета. Если для этого нет денег, то возможен поиск партнера для слияния.
5. Наиболее значительные активы компании или предприятия переводятся в дочерние структуры. В итоге эти дочерние компании отделяются от материнской, а агрессор покупает "пустышку".
6. Если агрессора интересует именно участие в производственной цепочке, то, не имея возможности договориться с менеджером или собственниками

предприятия, он пытается его купить. Возможно, целесообразно будет разрешить пользоваться активами, разобравшись в ситуации, за то, что пакет акций будет возвращен.

7. PR-защита. Формирование имиджа компании. Если компанию поглощают, а власти решат ее поддержать, то шансы агрессора существенно уменьшаются. Организация информационной войны против агрессора.

8. Проведение закрытой эмиссии акций с закрытым размещением.

9. Компания заключает договора с приложениями, которые вступают в силу в случае, если кто-то получает контроль над ней, и резко ухудшают общее финансово-экономическое состояние компании. В этом случае агрессор рискует получить множество штрафов и долгов.

10. Сознательное "навешивание" долгов на предприятие.

11. В случае если агрессора интересует не вся компания, а какая-то группа оборудования, система продаж, то такой актив можно вывести за пределы предприятия, выделить его в отдельную компанию, а в дальнейшем отделить от материнской компании. Если такого актива у предприятия нет, то интерес к поглощению у агрессора пропадает.

12. Поскольку самым распространенным методом поглощения в России является скупка долгов, то нужно попробовать договориться с кредиторами.

5.5 Реструктуризация в России как защита от поглощения

Выстроить грамотную систему защиты бизнеса от поглощения – вполне реальная задача. Это доказано практикой. Для этого нужно иметь опыт использования широкого спектра инструментов и приемов враждебного поглощения, опыт защиты от них, и понимание того, каким образом данное конкретное предприятие может быть поглощено.

Инструменты, используемые в процессе поглощения, имеют несколько уровней сложности, зависящих от стартовой позиции, занимаемой агрессором (отколовшийся от коалиции крупный собственник, миноритарный акционер, способный поставить под свои знамена значительное число акций, крупный кредитор, конкурент в лице влиятельной финансово-промышленной группы и т.п.). На каком уровне выступит агрессор, потенциальная жертва в большинстве случаев вполне может спрогнозировать. Соответственно, защита от поглощения должна строиться на том уровне, с которого ожидается нападение. Однако, если защита сработала на одном уровне нападения, агрессор может повысить уровень сложности, например, осознав бессмысленность атак на юридически безупречную систему защиты, обратиться к использованию административного ресурса. К этому нужно быть готовым.

Основной принцип, которым следует руководствоваться при выстраивании системы защиты, таков: прочность конструкции должна обеспечиваться не только юридической чистотой ее построения, но и наличием встроенных механизмов поддержания жизнеспособности системы, когда она подвергается штурму и, все же, частично разрушается.

Можно проиллюстрировать этот принцип следующим примером: реструктуризация проведена таким образом, что производственное предприятие, лишенное собственного сбытового подразделения, реализовывает всю

производимую продукцию через дилера, с которым заключено эксклюзивное соглашение. Дилер, естественно, на 100% принадлежит основному собственнику производственного предприятия. При этом собственник уверен, что в его бизнес защищен «отравленной пилюлей», и никто на его производство не покусится. Но агрессор все же появляется, и хотя юридическая чистота дилерского соглашения сомнений не вызывает, у него в руках, откуда ни возьмись, – исполнительный лист с запретом дилеру продавать продукцию предприятия. Один удар – и предприятие остается без сбыта, договор-то эксклюзивный, через другие фирмы или самостоятельно продукцию сбыть невозможно.

Безусловно, есть механизмы, позволяющие от этого удара защититься. Тем не менее, подобные элементы в корпоративной структуре при нанесении в них удара способны распространить паралич на весь бизнес в целом.

Принцип поддержания жизнеспособности при частичном разрушении системы универсален, он относится ко всем методам защиты от поглощения, но полнее всего раскрывается в отношении одной из наиболее эффективных и изящных мер – реорганизации бизнеса в корпоративную структуру такого типа, которая позволит резко усложнить задачу агрессору, а то и вовсе сделать ее невыполнимой.

Возможности, предоставляемые комплексом мер под общим названием «реструктуризация», позволяют значительно снизить угрозу враждебного поглощения для практически любой корпорации. Проблема в том, что для корпораций определенного типа применим лишь ограниченный круг таких мер. Скажем, менеджмент крупного приватизированного предприятия с распыленной структурой собственности не может позволить себе реструктуризацию того масштаба, которую проведут владельцы более 75% акций среднего по размерам предприятия.

Факторами влияния здесь выступают численность персонала и зависимость местного бюджета от налоговых поступлений с предприятия, структура собственности (степень концентрации, доля участия государственных и муниципальных органов), структура имущества (возможность разделения имущественного комплекса на части без существенных затрат) и др.

Тем не менее, реструктуризацию в том или ином виде можно провести на любом предприятии. Если даже предприятие подпадает под влияние перечисленных факторов, более действенного инструмента для повышения защищенности бизнеса от угрозы НТ (*hostile takeover*, (англ.) враждебное поглощение), чем реструктуризация, владельцам не найти.

Сравнивая издержки проведения реструктуризации с оценкой преимуществ повышения безопасности бизнеса, владельцы предприятий, в особенности тех, возможности проведения реструктуризации которых серьезно ограничены, часто делают выбор в пользу сохранения статус-кво. Причин этому можно привести, по крайней мере, две.

Во-первых, владельцы сталкиваются с психологическими сложностями соотнесения реальных издержек на реструктуризацию и гипотетических издержек борьбы с возможным агрессором. А во-вторых, любое серьезное предприятие инвестирует в поддержание покровительственных отношений местной или региональной власти, и признавать, что этого недостаточно, означает признавать ограниченную эффективность осуществлявшихся в течение многих лет инвестиций.

Причем вторая из указанных причин на практике встречается чаще. Преграда, называемая социологами *path dependence*, (с англ. - зависимость от однажды выбранного пути), является основным фактором, не позволяющим владельцам предприятий перейти на более эффективные методы защиты бизнеса.

Помимо цели повышения защищенности бизнеса от враждебного поглощения, в ходе реструктуризации можно добиться целей оптимизации налогообложения, минимизации хозяйственных рисков, улучшения качества управления корпорацией и выстраивания сбалансированной структуры собственности.

Безусловно, оптимальный экономический эффект может быть достигнут, только если базовой целью устанавливается налоговая оптимизация. Однако в планируемых нами программах реструктуризации это, все же, побочные цели, обеспечение непротиворечивости которых с базовой целью есть необходимое условие. Здесь проблема опять же упирается в то, что на предприятиях с ограниченными возможностями реструктуризации и экономическая эффективность реструктуризации заметно ниже, однако она есть, и при такой концепции реструктуризации владельцы бизнеса охотнее соглашаются на ее проведение.

Часто бывает, что некая «реструктуризация» на предприятии уже давно проведена. Обычно, это просто перемещение центра прибыли с основного производственного подразделения корпорации на компании-дилеры. Это достаточно действенный инструмент получения менеджерами-собственниками дохода от принадлежащего им бизнеса.

Такая ситуация отражает преобладание краткосрочных целей в отношении предприятия со стороны собственников, потому что в этом случае рассчитанная по денежному потоку цена самого производственного подразделения резко снижается. Возможному агрессору требуются гораздо меньшие финансовые затраты на аккумуляцию крупного пакета акций, т.е. явная недооцененность акций основного предприятия приводит к удешевлению покупки компании агрессором. В то время как добиваться нужно прямо противоположного.

Отсюда еще один принцип реструктуризации: стоимость находящихся в свободном обращении акций должна быть завышена по отношению к приходящейся на них доле в стоимости активов предприятия. Другими словами, если с предприятия выводится прибыль, с него должны быть выведены и активы.

На большинстве средних и крупных приватизированных предприятий структура собственности такова, что от 5 до 40 процентов акций распылено среди мелких держателей: работников и бывших работников предприятия. Дивиденды им если и начисляются, то копеечные, поэтому реальной ценности для держателей эти акции не представляют. Цена, по которой они готовы свои акции продать обычно исчисляется не в рублях за акцию, а в рублях за пакет, а решение продать базируется на том, превышает ли цена за пакет психологически важный уровень для держателя, до достижения которого соображения о сохранении собственности «на всякий случай» еще сильны.

Если основной собственник скупить сильно распыленную часть акций по каким-то причинам не может, необходимо создать предпосылки к тому, чтобы акции обрели реальную ценность, т.е. превратить их в нормально функционирующий финансовый инструмент. Выплачивая дивиденды в таком размере, чтобы их актуализированная стоимость превышала стоимость

приходящихся на одну акцию активов предприятия, можно добиться того, что даже не ориентирующийся в финансовой математике акционер продаст акции агрессору лишь по завышенной цене.

Альтернативный вариант предполагает занятие еще более жесткой позиции: принятие решения о том, что сохранение основной массы активов на балансе юридического лица, созданного в ходе приватизации является источником постоянного риска, а потому, не допускается. Во-первых, существует опасность того, что приватизационные сделки будут оспорены, во-вторых, акции именно этого лица находятся в свободном обращении, т.е. потенциальный агрессор сможет приобрести долю собственности на основные средства предприятия.

Необходимой в таком положении мерой является проведение реорганизации общества путем выделения (с сохранением юридического лица-носителя торговой марки) или разделения (с предварительным переводом прав на торговую марку на подконтрольную компанию). Это осуществимо, если совокупный контроль заинтересованных в реструктуризации лиц достигает 75% акций. Если контроль на уровне 50% акций, можно использовать вариант внесения части имущества в уставный капитал вновь создаваемой компании (рекомендуется на всякий случай заручиться одобрением общего собрания акционеров), причем предприятие, из которого таким образом выводятся активы, должно стать мажоритарным участником.

Первый путь можно использовать для того, чтобы пропустить мелких акционеров через сито, отсеивающее тех, кто согласится на выкуп их акций обществом, и тех, кто предпочтет обменять свои акции на доли участия во вновь создаваемых компаниях. Устройство этого сита может быть таким, что на выходе структура акционерного капитала будет гораздо более приближена к желаемой.

Для тех, кто склонился ко второму варианту, существует несколько способов постепенного снижения доли участия материнского предприятия в капитале дочки. Единственный принцип, которого нужно придерживаться в такого рода операциях: все инициативы по изменению структуры капитала должны исходить от стороннего инвестора, задача материнской компании – бездействовать.

Этот принцип должен реализовываться на всех уровнях действий по снижению доли материнской компании: внесение предложения в повестку дня общего собрания участников, голосование по этому вопросу, оплата доли и т.д. Вывод активов из предприятия достаточно легко квалифицируется как уголовно наказуемое деяние, поэтому при осуществлении таких действий необходимо на каждом мало-мальски значимом этапе демонстрировать безынициативность и незаинтересованность руководства материнской компании. Тогда уголовное дело будет лишено судебной перспективы.

Хорошо известен давно сформулированный принцип реструктуризации, в соответствии с которым имущество и риски должны быть разнесены по разным юридическим лицам, т.е. бизнес нужно структурировать так, чтобы компании-владельцы имущества не вели хозяйственной деятельности, а компании-трейдеры, соответственно, не владели имуществом. Так вот, следующий принцип реструктуризации состоит в том, чтобы использовать для создания всех структурных единиц, будь то компании-владельцы активов или компании-трейдеры, организационно-правовые формы, правила управления и ведения деятельности в

которых в большей степени определяются внутренними документами компании, нежели нормативно-правовыми актами.

Чем меньше регулирующие органы вмешиваются во внутренние дела компании, непосредственно, или путем издания нормативных актов, тем больше простор для маневра. К тому же оспаривать в судах решения, принятые в соответствии с внутренними правилами компании на порядок сложнее, чем, если они приняты по процедуре, прописанной в законе или иных правовых актах. К таким формам, в частности, относятся общество с ограниченной ответственностью и автономная некоммерческая организация.

Вопросы для повторения темы:

1. Перечислите основные этапы процесса слияния и поглощения.
2. Какие параметры должны учитываться руководством фирмы, если в процессе слияния или поглощения предполагается выход на новые рынки?
3. Перечислите основные стратегии присоединения и раскройте их содержание.
4. Какой практический интерес представляет изучение истории фирмы?
5. На что обычно указывает ослабление контроля фирмы за своим Интернет-сайтом?
6. Какие выводы о стратегии компании можно сделать, зная каких внешних консультантов она привлекает?
7. Назовите пять ключевых категорий, разработанных специалистами консалтинговой компании Accenture, для оценки слияний и поглощений.
8. Что Вы понимаете под защитой от «недружественного поглощения»?
9. Раскройте сущность методов супербольшинства и справедливой цены, существует ли между ними связь?
10. Перечислите основные виды «ядовитых пилюль»?
11. Назовите основные сходства и различия Flip-over plan и Flip-in plan.
12. Назовите основное отличие Back-end plan от Flip-out plan.
13. Раскройте сущность метода рекапитализации высшего класса.
14. Что представляет собой «реструктуризация активов», с какой целью она производится?
15. Назовите основные отличие между способами защиты от недружественного поглощения «Белый рыцарь» и «Белый сквайр».
16. В чем состоит основной недостаток защиты Пэкмена?
17. Какие стартовые позиции, занимаемые агрессором, Вы знаете?
18. Сформулируйте основной принцип проведения реструктуризации.

Литература:

1. Камышанский В.П. «Право собственности: переделы и ограничения», М., Юнити; 2000
2. Ментюкова С.С.; Статья «Слияние и поглощения в пищевой промышленности»; Журнал «Слияние и поглощения» №2; 2003.
3. Никиткин Л.Л., Д.В. Нуржинский. « Стратегия и тактика защиты от недружественного поглощения».

4. Радыгин А.Д., Энтов Р.М. (1999) “Институциональные проблемы развития корпоративного сектора: собственность, контроль, рынок ценных бумаг.” Москва, ИЭПП.

5. Радыгин А.Д., Энтов Р.М. "Корпоративное управление и защита прав собственности: эмпирический анализ и актуальные направления реформ", Москва, 2001., ИЭПП.

6. Храброва И.А. «Корпоративное управление», Москва ,ИД «Альпина».

7. Шапуров Д.В. статья «Реструктуризация корпорации» Журнал «Слияние и поглощения» №2; 2003.

Глава 6 Экономическая безопасность на рынке ценных бумаг

Ключевые понятия:

Рынок ценных бумаг
Ценная бумага
Мошенничество
Аналитики продавцы
Аналитики покупатели
Независимые аналитики
Стоп-лист
Бронзовый вексель
Встречный вексель
Эмиссия
Реестр
Трансфер-агент
Депозитарная деятельность
Недобросовестная торговля
Манипулирование рынком
Инсайдеры
Спекуляция

6.1 Общие положения

Рынок ценных бумаг в общем виде можно определить как совокупность экономических отношений по поводу выпуска и обращения ценных бумаг.

Гражданский кодекс РФ определяет **ценную бумагу** как документ, удостоверяющий с соблюдением установленной формы и обязательных реквизитов имущественные права, осуществление или передача которых возможны только при его предъявлении. На этом рынке осуществляется обращение ценных бумаг, заключение гражданско-правовых сделок, влекущих переход прав собственности на ценные бумаги.

На сегодняшний день одной из важных задач, стоящей перед государством, является обеспечение экономической безопасности на рынке ценных бумаг, так как отсутствие надежного механизма защиты рынка ценных бумаг приводит к росту преступлений и мошенничеств. Имеющиеся материалы и судебная практика свидетельствуют о том, что преступные группировки активно осваивают формирующийся фондовый рынок. Существенную помощь в этом им оказывают связанные с ними руководители банковских структур.

Преступления, посягающие на интересы владельцев ценных бумаг, характеризуются повышенной общественной опасностью в связи с тем, что наносят ущерб как участникам рынка, так и экономике в целом, увеличивая инвестиционные риски и ухудшая инвестиционный климат.

Обеспечение безопасности на рынке ценных бумаг можно определить как совокупность законодательных, правоприменительных и регулирующих мер,

принимаемых государством и институтами. Оно должно осуществляться на федеральном уровне, на уровнях субъектов Федерации и участников рынка ценных бумаг. Способность государства защитить рынок от негативных воздействий и не допускать различного рода мошеннических операций является основной характеристикой состояния безопасности рынка ценных бумаг.

Мошенничество в Уголовном кодексе РФ определяется как преступление, связанное с хищением чужого имущества или приобретением права на чужое имущество путем обмана или злоупотребления доверием. Мошенничество является формой хищения. Формы мошеннического обмана весьма разнообразны.

Российскими юристами определен основной состав правонарушений на рынке ценных бумаг, структура которого представлена на рисунке 6.1.

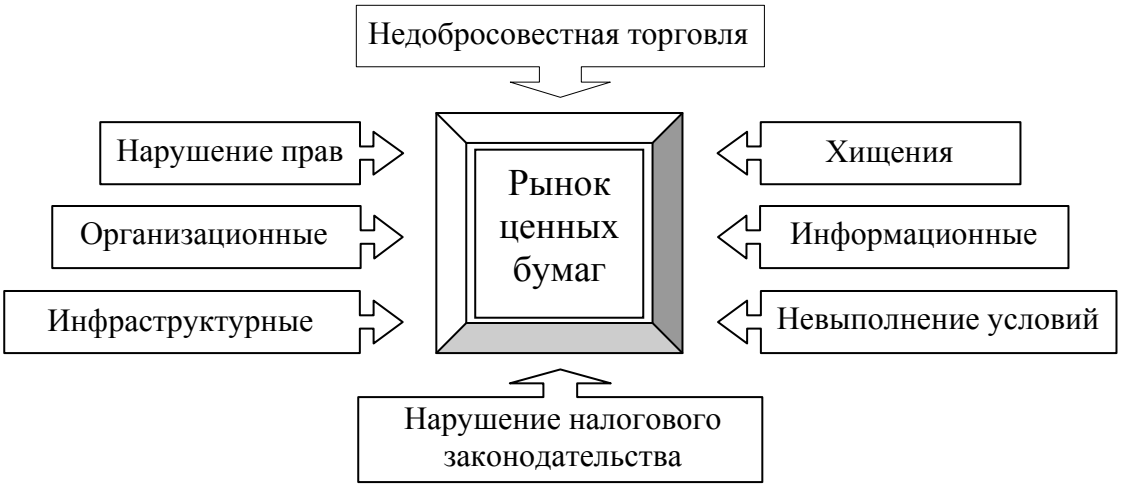

Рисунок 6.1 - Основной состав правонарушений на рынке ценных бумаг

1. Информационные:

а) недобросовестное информирование инвесторов о доходности, ликвидности, сокрытие других важных сведений о ценных бумагах;

б) неполное раскрытие информации эмитентом о своей компании и ее ценных бумагах;

в) нераскрытие профессиональным участником информации о себе с точки зрения компетентности и надежности.

2. Инфраструктурные, связанные с риском хранения и учета ценных бумаг:

а) отказ от внесения в реестр собственных ценных бумаг;

б) использование ценных бумаг собственника, переданных на хранение, без его согласия.

3. Невыполнение условий сделок с ценными бумагами.

4. Нарушение прав акционеров, в том числе злоупотребления администрации предприятия или группы акционеров.

5. Хищение денежных средств или ценных бумаг партнера по сделки или инвестора, мошенничество, а также подделка ценных бумаг.

6. Организационные:

а) невыполнение требований контрольных государственных органов;

б) нарушение стандартов деятельности профессиональными участниками;

в) нарушение стандартной эмиссии эмитентом.

7. Нарушение налогового законодательства при совершении сделок с ценными бумагами.

8. Недобросовестная торговля.

6.2 Информационные правонарушения на рынке ценных бумаг

В состав информационных правонарушений на рынке ценных бумаг включают:

1. Недобросовестное информирование инвестора о доходности, ликвидности, сокрытие других важных сведений о ценны бумагах;
2. Неполное раскрытие информации эмитентом о своей компании и ее ценных бумагах;
3. Нераскрытие профессиональным участником информации о себе с точки зрения компетентности и надежности.

Наиболее распространенным информационным правонарушением является ввод в заблуждение инвесторов аналитиками.

Как известно, фондовые аналитики делают обзор инвестиционной привлекательности ценных бумаг вовсе не для собственного удовольствия - этим они зарабатывают себе деньги. При этом в своих отчетах они дают недвусмысленные рекомендации по покупке или продаже тех или иных ценных бумаг, т.е. помогают зарабатывать деньги инвесторам. В том случае, если мнение авторитетного аналитика широко растиражировано по ТВ, электронным и печатным СМИ, оно способно оказать существенное влияние на рынок акций конкретной компании. Возможность манипулирования рынком и наличие конфликта интересов у его участников могут иметь крайне негативные последствия.

Аналитики могут работать непосредственно на инвестиционные компании и банки, оказывающие услуги эмитентам ценных бумаг, по которым выдаются рекомендации, или на самих эмитентов. В других случаях аналитики могут прямо или косвенно владеть ценными бумагами. В целом аналитиков подразделяют на три условных категории:

Аналитики продавцы – работающие на инвестиционные банки и компании, которые оказывают брокерские услуги сторонним инвесторам.

Аналитики покупатели – работающие на взаимные и хеджевые фонды, которые покупают ценные бумаги для себя.

Независимые аналитики – работающие только на себя и продающие клиентам свои обзоры по подписке или на заказ.

В каждом случае возможны ситуации, сопряженные с конфликтом интересов у действующих сторон. Так, при размещении ценных бумаг на рынке все участники: андеррайтер, эмитент и аналитик, прямо заинтересованы в позитивных рекомендациях. Андеррайтеру это нужно для успешного размещения конкретного выпуска и поддержания котировок, а также укрепления репутации для привлечения следующих клиентов. Эмитент заинтересован в привлечении денег и уменьшении стоимости привлекаемого капитала, а также в росте котировок своих акций. Что касается аналитика, то его компенсация и бонусы часто напрямую зависит от объема операций профессионального участника. Негативный отчет может сорвать выпуск бумаг, подмочить репутацию андеррайтера или привести к потере клиента и убыткам.

При оказании брокерских услуг, компания может не брать деньги с клиентов за свои аналитические обзоры. Однако рекомендация “покупать” привлекает новых клиентов и увеличивает комиссионные сборы. Поэтому брокерам выгодно чаще давать рекомендации на покупку, чем на продажу. Более профессиональные инвесторы это понимают и интерпретируют рекомендацию брокерских компаний “держать” как сигнал к продаже.

Аналитики и инвестиционные компании крайне редко рекомендуют продавать бумаги, которыми владеют непосредственно, через опционы или косвенно. В 2003г., по данным **SEC** (комиссия по ценным бумагам и биржам в США), рекомендации к продаже давались менее чем в 1% случаев, когда аналитики были лично заинтересованы в росте котировок.

Например, год назад в Америке аналитические службы 10 крупнейших компаний (Citigroup, Credit Suisse First Boston, Merrill Linch, Morgan Stanley, Goldman Sachs, Bear Stearns, JP Morgan Chase, Lehman Brothers, UBS Warburg, U.S. Bancorp Piper Jaffray) были обвинены в том, что их аналитики вводили в заблуждение инвесторов, публикуя тенденциозные исследования об акциях. Одни составляли жульнические аналитические отчеты, другие втайне получали плату от клиентов, третьи – выделяли акции «горячих» IPO руководителям компаний-клиентов. В конечном итоге компании были вынуждены заплатить рекордный штраф на общую сумму $1.4 миллиарда.

Особо «отличившиеся» были наказаны персонально. Так, Джэк Грубмен из Citigroup согласился заплатить штраф в $1.5 млн. и был пожизненно лишен права заниматься аналитической деятельностью для инвесторов. Грубмена обвиняли в том, что он предоставлял клиентам заведомо ложную информацию и уговаривал их покупать акции компаний, у которых были серьезные проблемы с финансированием долгов. У Грубмена на Уолл-Стрит всегда была безупречная репутация, ему доверяли. Причем, как показало расследование, действия аналитика были продиктованы прямыми указаниями основателя и генерального директора компании Сенфорда Уэйла. После оптимистичных прогнозов аналитика ценные бумаги AT&T взлетели на 5-7%. Citigroup на волне покупательского ажиотажа успешно реализовала свой пакет акций AT&T, после чего Грубмен тут же снизил рейтинг до «нейтрального». Финансовое положение AT&T скоро перестало быть тайной, и инвесторам осталось только подсчитывать убытки.

В прессе иногда появляются статьи, посвященные конфликту интересов российских андеррайтеров. Андеррайтеры рекомендуют инвесторам бумаги своих клиентов, хотя иногда и добавляют для компании прочих эмитентов. Кроме того, в России легко может использоваться рекомендация “не покупать”, причем основанная не на объективном анализе финансового состояния эмитента, а на одном лишь желании навредить конкуренту.

В отличие от ситуации с размещением ценных бумаг, когда андеррайтер хорошо известен, при обычной торговле ценными бумагами заметить конфликт интересов несколько сложнее. Однако и здесь бросаются в глаза некоторые закономерности. Так, аналитики “НИКойла” никогда не позволят себе даже намека на критику ЛУКОЙЛа, не говоря уже о рекомендации к продаже акций компании. Наоборот, для компаний-конкурентов всегда найдутся аргументы, подтверждающие их переоцененность по сравнению с ЛУКОЙЛом.

Так, в 2002 году фантастический рост капитализации “Сибнефти” все-таки расколол стройные ряды оптимистов фондового рынка. “Тройка диалог”, “Пролог” и “Атон” оценивали “справедливую цену” акции компании соответственно в 1,15, 1,5 и 1,6 долл. США. При стоимости акций этой компании, которая в то время была чуть ниже 2 долл. это означало рекомендацию к продаже. В то же время Brunswick считало справедливой цену 2,4 долл., а “НИКойл” – 2,2. В чем причина такого расхождения? В случае с Brunswick это был конфликт интересов – компании недавно выступила менеджером размещения 1,26% уставного капитала “Сибнефти” институциональным инвесторам, ей выгодно было подогреть рынок. Тем более, что для этого были все возможности, т.к. Brunswick - одна из крупнейших компаний по объему операций на российском фондовом рынке, а реальная доля акций “Сибнефти” в свободном обращении была очень мала, скорее всего, гораздо меньше заявленных 12%.

6.3 Хищение денежных средств или ценных бумаг партнера по сделке или инвестора, мошенничество, а также подделка ценных бумаг

6.3.1 Организация «пирамид»

Одним из видов мошенничества является организация так называемых «**пирамид**» (в западных странах они известны как «схема Понзи») - это построение по типу краткосрочного домика, приносящее мошенническим путем огромные проценты, выплачиваемые первоначальным инвесторам за счет вовлечения в программу новых инвесторов, которые в итоге теряют все или почти все деньги в пользу организатора этой операции.

Движущей силой подобных «пирамид» является взрывоподобное развитие финансовых услуг, в первую очередь рынка ценных бумаг и новых инвестиционных возможностей, которые представляются населению. Организаторы «пирамид» постоянно придают своим операциям все новые обличья с тем, чтобы их труднее было распознать. Мошеннические фирмы функционируют в юрисдикциях и странах, отдаленных от места нахождения клиентов, например в оффшорных зонах; используют службы почтовых отправлений, телефонные службы и почтовые ящики для сокрытия данных о себе или для создания ложного впечатления о значительности проводимой операции.

Так, в начале лета 2003 года в Бруклине состоялся суд над сотрудниками фиктивной брокерской компании, которая действовала более пяти лет. Из карманов полутора тысяч человек из 14 стран мошенники «выудили» более $100 миллионов.

Аферой руководил российский гражданин Андрей Кудашев, создавший две компании: Evergreen International Spot Trading и «независимую» от первой, расчетную компанию First Equity Enterprises. При помощи них Кудашев и его компании обирали потенциальных инвесторов. Более 150 брокеров Evergreen International Spot Trading обзванивали клиентов и советовали вложить свои деньги в валютные торги. Естественно, сделать это надо было через First Equity Enterprises. Клиентам обещали весьма достойную прибыль – 25-30% годовых – и предоставляли гарантии Chase Manhattan Bank. Клиенты не подозревали, что банк отказал обеим «русским» компаниям и закрыл их счета.

В одном из рекламных проектов утверждалось, что First Equity Enterprises создана в 1971 году и «ежедневно осуществляет операции для центральных и

коммерческих банков в таких колоссальных масштабах, что ваш капитал почти идеально ликвиден». В случае нарастающих убытков инвесторам гарантировалось, что операции с их средствами будут автоматически прекращены. Клиенты регулярно получали отчеты из Evergreen, в которых фигурировали их мифические прибыли. Если кто-то из них хотел забрать свои деньги, ему переводили сумму, взятую из средств новых инвесторов. На средства вкладчиков приобреталась недвижимость, антиквариат, меха и ювелирные украшения.

Чтобы распознать подобные «схемы» и «пирамиды» следует руководствоваться некоторыми практическими рекомендациями:

1. Опасайтесь обещаний высоких гарантированных прибылей;
2. Избегайте организаторов, которые не дают четких и подробных разъяснений в отношении своих инвестиционных механизмов;
3. Проверяйте информацию, касающуюся организатора операции;
4. Получите информацию о выпуске ценных бумаг в ФКЦБ РФ;
5. Запрашивайте подробную информацию в письменной форме;
6. Не поддавайтесь давлению и не осуществляйте реинвестирования, пока вы не получите ваших прибылей;
7. Отмечайте поведение, не соответствующее правилам ведения бизнеса или нарушения в ходе предоставления услуг.

6.3.2 Подделка ценных бумаг

Распространены также мошенничества в качестве подделки ценных бумаг. Ценная бумага считается неподлинной («фальшивой») из-за утраты юридической основы вследствие:

1. Наличия дефектов формы, определенной соответствующими нормативными документами;
2. Несоответствие представленной ценной бумаги подлинному образцу по комплексу технологических особенностей.

Следовательно, существуют следующие виды подделок:

1. Дефекты формы ценных бумаг;
2. Частичная подделка;
3. Полная подделка.

Наиболее часто встречаются подделки векселей. Многие банки выпускают веселя для обслуживания юридических лиц. Обращение различного рода векселей, как надежный способ замены «живых» денег и удобный метод укрытия доходов от государственного налогообложения занимает сейчас прочное место на фондовом рынке. Кроме того, вексельный оборот является основным при расчетах в «теневом» секторе экономики, оплате неучтенной продукции и услуг.

Рассматривая финансовые мошенничества с использованием векселей, можно условно выделить два направления:

- Обман со стороны векселедателя (**трассанта**);
- Обман со стороны векселедержателей, а также третьих лиц.

Наиболее распространенным является мошенничество со стороны векселедателя. При этом используется то обстоятельство, что вексельные отношения являются строго формальными денежными обязательствами, в связи, с чем даже небольшие дефекты формы влекут его недействительность. Поэтому изготовление бланков векселей с нарушением технических требований, заведомо

неправильное их оформление не позволяет держателям своевременно их опротестовывать и получать по ним средства.

Дефект формы заключается в отсутствии обязательных реквизитов ценных бумаг или несоответствии ценных бумаг установленной для нее форме.

Чаще всего дефекты формы появляются в векселях, при этом отмечено следующее:

- отсутствие так называемой «вексельной метки» в тексте документа;
- написание слова «вексель» и текста самого документа на разных языках;
- отсутствие даты составления векселя и подписи векселедателя или подлог подписи;
- отсутствие предложения (обещания) уплатить определенную сумму конкретному лицу;
- некорректное (неконкретное) указание суммы платежа;
- различия в наименовании векселедателя в тексте и заверяющих реквизитах и т.д.

Факт дефекта формы может быть установлен только судом, что увеличивает число мошенничества с ценными бумагами.

Например, в конце 90х годов группой мошенников были попытки получения кредита в ряде коммерческих банках под залог так называемых «Золотых векселей». Указанные векселя были составлены с дефектами формы, в частности, в них была указана неопределенная сумма платежа: «в размере, эквивалентном стоимости 10000 грамм химически чистого золота, определенной Роскомдрагмет РФ на момент погашения этого векселя».

Дефектом формы может также выступать подлог подписи или неправильное оформление подписей должностных лиц в этих документах. Для подлога подписи кто-либо из заместителей уполномочивается подписывать векселя по доверенности. Далее доверенность уничтожается. При предъявлении к оплате векселя представляются как подписанные неуполномоченным лицом. Подпись, выполненная неуполномоченным лицом, ни к чему не обязывает лицо, от имени которого подпись поставлена. Векселедателем признается гражданин, поставивший подпись. Розыск данного гражданина, как правило, не приводит к успеху.

Встречаются документы, в которых вместо собственноручной подписи соответствующего руководителя наносится его факсимиле; кроме того, подписи и другие реквизиты на очень высоком качественном уровне могут быть воспроизведены с помощью современного полиграфического и копировально-множительного оборудования.

Так, известны случаи, когда фальшивые векселя одного из крупных банков при осуществлении сделки для проверки предъявлялись эмитенту и там признавались подлинными, в том числе и подписи и даже теми лицами, от имени которых они были поставлены. Преступники для большего сходства подбирали пишущие средства, мало отличающиеся по цвету от тех, которыми ставились подписи на подлинных векселях.

Но подлинность бланка, подписей и оттисков печати не дает 100%-ю гарантию от неприятностей, если преступник подделал (внес изменения в) текст или реквизиты ценной бумаги. Например, один из наиболее простых вариантов подобных мошеннических операций – это изменение номера похищенной бумаги с целью исключить подозрение при проверки по «**стоп-листу**».

Для именных ценных бумаг подобные случаи не имеют принципиального значения, так как передача прав на их владение оформляется у эмитента по приказу их владельца. Для ордерных ценных бумаг такой способ воспроизведения подписей и оттисков печатей таит потенциальную опасность их подделки и махинаций с ними.

Особую опасность представляют поддельные ценные бумаги с высокой обозначенной стоимостью. Если номинал оного векселя равен 1 млн. руб., то приобретение даже одной такой ценной бумаги может нанести существенный ущерб купившей ее организации. Ведь высокая обозначенная стоимость бумаги позволяет преступникам затратить на ее изготовление значительные средства и усилия и в результате получить высококачественную подделку.

Существуют и достаточно простые «фальшивки», изготовленные с помощью полноцветной копировальной техники, на которых плохо имитированы или вообще отсутствую основные элементы защиты (микротекст, люминесенция и пр.). Обнаружить такие бумаги можно, имея минимальные знания в этой области и простейшие технические средства.

Для граждан, получивших недоброкачественные векселя, практически исключена возможность гражданско-правовой защиты интересов. Единственной гарантией возврата средств может явиться уголовное преследование. Данные деяния могут квалифицироваться как мошенничество.

Наряду с этим векселя могут выпускаться банкротами, неплатежеспособными банками, предприятиями, фирмами. Как правило, такие векселя продаются в отдаленных районах, что затрудняет проверку финансово-хозяйственной деятельности векселедателя. Кроме того, порой векселя выпускаются неюридическими лицами (филиалами, представительствами и т.п.), что дает возможность в дальнейшем уклоняться от их оплаты под предлогом превышения полномочий лиц, их подписавших.

Возможна также полная подделка векселей. В этом случае мошенники изготовляют точную копию бланка векселя от имени фирмы, выпускающей векселя. Затем с помощью сканера изготовляют передаточные надписи и продают их юридическим и физическим лицам, которые не смогут получить по ним причитающиеся средства. Преступниками для проведения крупномасштабных коммерческих операций используются подлинные бланки веселей сбербанка России, ксерокопии векселей Главного управления федерального казначейства министерства финансов России. В различных регионах периодически появляются фальшивые векселя на несколько миллионов каждый, от имени некоммерческих структур различных организационно-правовых форм.

Платеж по векселю может быть обеспечен посредством поручительства (**аваля**). Такое поручительство обычно дается банком как за векселедателя, так и за каждого другого, обязанного по векселю лица. В ряде случаев мошенники подделывают аваль.

Также встречаются преступления, совершаемые потенциальными приобретателями векселя:

1. **Хищение векселей из депозитария.** Большую часть ценных бумаг, в том числе и векселей, владельцы, не желая подвергать себя дополнительному риску, хранят в депозитариях (специализированных хранилищах) различных коммерческих банков. Однако при определенных обстоятельствах депонирование векселей может

облегчить их хищение. Сущность данной схемы состоит в заключении от имени фиктивного предприятия договора на приобретение векселей на выгодных для продавца условиях, депонировании их в депозитарии банка и последующем их хищении посредством использования фальсифицированных документов. Хищение становится возможным вследствие нарушения порядка депонирования векселей в депозитарий, когда передача векселей осуществляется совместно с предыдущим держателем. При этом последний получает доступ к информации, которая должна быть конфиденциальной (количество, номиналы, номера векселей, реквизиты юридической фирмы, копии документов с оттисками печатей предприятия и подписями должностных лиц). Используя указанные данные, мошенник изготавливает необходимый набор документов, позволяющих завладеть находящимися на хранении в депозитарии векселями. Похищенные векселя реализуются по существенно заниженной цене, а организаторы и исполнители преступления скрываются.

Основными характеристиками совершения рассмотренного мошенничества являются:

а) большая поспешность составления и подписания договора;

б) отсутствие такого важного элемента проверки партнера по сделке, как установление места его прописки и проживания (а при такой проверке - невозможность их установления);

в) потенциально значительная экономическая выгода для стороны, продающей векселя, и обещание выплаты больших вознаграждений всем посредникам и участникам сделки;

г) необоснованные попытки присутствия мошенников при составлении и подписании договора, который их непосредственно не касался (договор о хранении векселей), с целью выяснения системы оборота документов, особенностей хранения и учета ценных бумаг;

д) использование для облегчения вхождения в доверие к владельцам векселей депозитария как якобы гарантии безопасности совершения сделки.

2. **Мошенничество с использованием “серых” схем расчетов**. Суть схемы состоит в том, что мошенники провоцируют покупателя на “серые” схемы расчетов, а затем законным способом возвращают себе векселя. Например, группа мошенников, имея на руках ликвидные векселя на солидную сумму (на практике обычно это были векселя Сбербанка погашением “по предъявлении”), предлагает их по интересной для участников рынка цене. Рассчитываться за них предлагается за наличный расчет (а сумма сделки в сотни раз превышает допустимый законом уровень). Торг по цене идет до того уровня, пока один из участников рынка (например, небольшая компания), не согласится на эту схему. Далее векселя проверяются у эмитента и передаются без сопроводительных документов, подтверждающих законность их приобретения. В тот же день продавцы обращаются в органы внутренних дел с заявлениями о краже (или утрате) векселей.

3. **Искусственное раздувание спроса**. Суть схемы состоит в создание искусственного спроса на неликвидный вексель, который, под якобы имеющийся спрос и покупает, с целью перепродажи, наиболее доверчивый участник рынка, а затем, “покупатель” отказывается от сделки под каким-либо предлогом. Договор продажи при этом подписывается с фирмой, зарегистрированной по подложным документам.

Как уже упоминалось ранее, вексельное обращение все чаще используется для отмывания незаконных доходов и обслуживания финансового оборота в теневой экономике. Юридические лица для уклонения от уплаты налога путем погашения своей ссудной задолженности используют вексель, зачисляют средства не на расчетный, а на вексельный счет, списание с которого в бесспорном порядке не производится. Самый простой способ ухода от налогообложения с использованием векселя – постановка на векселе бланков индоссамента как вполне законного способа ухода от солидарной ответственности в случае протеста векселя. В Российской практике бланковый индоссамент стал способом превращения векселя в «черную» наличность, так как позволяет избежать обязательной постановки его на баланс того или иного юридического лица.

Очень часто для совершения преступления векселедатель вступает в сговор с одним из векселедержателей. При этом используются следующие способы:

1. **Выдача дружеского или встречного векселя**. Дружеские векселя передаются платежеспособным предприятием в качестве “дружеской услуги” другому предприятию, испытывающему финансовые затруднения и нуждающемуся в кредите (либо акцептуются векселя последнего), с тем, чтобы векселедержатель рассчитался со своими кредиторами либо учел его в банке. Криминальный аспект использования дружеских векселей состоит в том, что последние могут быть использованы для искусственного увеличения суммы долга векселедателя при признании его несостоятельным. Суммы, выплаченные по таким векселям, возвращаются затем векселедержателем векселедателю. Дружеские векселя выписываются обычно в случае наличия доверия к контрагенту. Однако в качестве гарантии от убытков, которые векселедатель может понести в случае неоплаты дружеского векселя, векселедержатель вручает своему контрагенту вексель на ту же сумму – встречный вексель.

2. **Выпуск и передача векселя, отвечающего всем формальным требованиям, однако заведомо не обеспеченного.** Его составителям и векселедателям заведомо известно, что оплачен он не будет потому, что у плательщика отсутствуют необходимые активы, и их появление не предвидится. Особую опасность представляют преступные операции с использованием необеспеченных векселей, осуществляемые организованными преступными группами под прикрытием законной банковской деятельности. Преступная деятельность маскируется под проведение сложных видов финансовых операций, направленных на погашение задолженности по налогам перед федеральным бюджетом.

3. **Выпуск бронзовых векселей**. Бронзовым, или дутым называется вексель, не имеющие реального обеспечения и выписываемые от имени несуществующей фирмы. В легальном бизнесе они используются с целью получения наличных денег в банке либо для осуществления платежа по сделке. Преступное их использование имеет целью мошенническое присвоение имущества посредством передачи по индоссаменту добросовестному приобретателю, авалирования и т.п. В результате наносится ущерб векселедержателям либо другим обязанным по нему лицам. Выявление преступлений, связанных с необеспеченными векселями достаточно сложно. Для подтверждения того факта, что подобные векселя оплачиваться не будут, необходимо дождаться, как минимум, указанного в них срока платежа и документально оформить процедуру предъявления их к оплате.

4. **Датирование векселя задним числом.** Целесообразно выделить две различные ситуации совершения данного преступления. В первом случае перенос даты составления векселя осуществляется без ведома первого приобретателя. Например, векселедатель хочет перенести дату составления векселя на период собственной недееспособности или отсутствия у него полномочий. Во втором случае датирование производится с ведома или по инициативе векселеприобретателя. Цель подобных действий - сокрытие имущества от требований кредиторов, увеличение суммы долга данного предприятия либо суммы долгов, сосредоточенных в руках определенных кредиторов. Датирование векселей задним числом создает видимость того, что они были выданы относительно давно, в период благополучной работы предприятия. Данные действия направлены на перераспределение имущества предприятия в преддверие банкротства в пользу одних лиц и в ущерб другим. Если датирование векселей задним числом направлено на увеличение долгов предприятия с целью спровоцировать объявление его банкротом, то налицо преднамеренное банкротство. Руководитель предприятия выдает векселя на подставных лиц, принимает решение об их оплате, производит оплату и скрывается с намерением впоследствии завладеть суммами, выплаченными по таким векселям.

5. **Оставление векселя в обращении после его оплаты**. Схема данного преступления выглядит следующим образом. Векселедежатель, получивший платеж, договаривается с векселедержателем, который этот платеж произвел, о том, чтобы последний не забирал у него вексель. Действуя в соответствии с договоренностью, векселедержатель предъявляет регрессный иск из факта неплатежа по векселю к индоссантам и авалистам. Для этого он совершает протест векселя и, имея на руках опротестованный вексель и акт о протесте, получает возможность взыскать всю сумму векселя еще раз с одного или нескольких должников в порядке регресса. Полученная сумма впоследствии делится между векселедателем и взыскателем. Совершение такого взыскания представляет собой мошенничество.

Особую опасность, как для рынка ценных бумаг, так и для экономики любой страны представляют производные ценные бумаги. Как известно, сделки с производными финансовыми инструментами делят на составные части риски, присущие лежащим в их основе финансовым активам; отделять эти риски и торговать ими отдельно от базисного актива. Деривативы, являясь инструментом страхования рисков для отдельных участников рынка, для других выступают исключительно как спекулятивный инструмент. При этом деривативы остаются инструментами, необеспеченными реальными активами, ведь в их основе лежат главным образом процентные ставки и курсы валют. В этом состоит их серьезная опасность. Имея тенденцию к неограниченному росту, обязательства по деривативам концентрируются у ограниченного круга крупных участников финансового рынка. В результате возникшие в силу тех или иных причин трудности с использованием обязательств одного из участников рынка могут за короткое время породить «эффект домино» и дестабилизировать рынок.

По мнениям многих экономистов, рынок производных финансовых инструментов таит в себе серьезные опасности, способные нанести существенный вред как финансовым системам развитых стран, где обращается основной объем производных инструментов, так и мировой экономике в целом.

Известный американский финансист У. Баффета полагает, что производные финансовые инструменты являются оружием массового поражения и несут катастрофические риски для мировой экономики. По его мнению, проблемы, связанные с ними, могут превратиться в системные, т.е огромные рыночные риски. Захеджированные производные инструменты в настоящее время сконцентрированы у относительно небольшого количества участников рынка. Если производные финансовые инструменты могут снизить риски отдельно взятого участника рынка, то в рамках финансовой системы они лишь перепадают на другого участника, выступающего противоположной стороной по контракту.

По состоянию на конец 2003 года общий объем обязательств семи банков – ведущих операторов рынка производных финансовых инструментов США превышал 50 трлн. долл. при размере их совокупного собственного капитала в 460млрд. долл. По оценкам специалистов, если бы Банк JP Morgan Chase потерпел убытка по 15%-там открытых позиций по производным финансовым инструментам, ему пришлось бы израсходовать весь свой собственный капитал для закрытия убыточных позиций.

Таким образом, негативное влияние на рынок ценных бумаг оказывают не только мошеннические операции, а также и законные действия самих участников рынка.

6.4 Организационные правонарушения

6.4.1 Злоупотребления в процессе эмиссионной деятельности

Эмиссионной является деятельность по выпуску ценных бумаг. Процедура эмиссии ценных бумаг включает, как правило, следующие этапы:

а) принятие эмитентом решения о выпуске эмиссионных ценных бумаг;

б) регистрацию выпуска эмиссионных ценных бумаг;

в) для документарной формы выпуска - изготовление сертификатов ценных бумаг;

г) размещение эмиссионных ценных бумаг;

д) регистрацию отчета об итогах выпуска эмиссионных ценных бумаг.

Выпуск в обращение ценных бумаг, не прошедших государственной регистрации. Совершение данных деяний повышает вероятность появления на рынке фондовых инструментов недобросовестных эмитентов, различных суррогатов ценных бумаг (билеты МММ), снижает доверие инвесторов, увеличивает инвестиционные риски и создает благоприятные условия для осуществления крупномасштабных мошеннических операций, наносящих ущерб инвесторам. В соответствии с действующим законодательством, выпуск в обращение ценных бумаг, не прошедших государственной регистрации запрещен. Он признается несостоявшимся. Сделки, совершаемые с данными ценными бумагами, являются недействительными.

Создание преимущественных условий приобретения ценных бумаг для отдельных категорий потенциальных инвесторов обусловлен стремлением эмитентов сохранить контроль над предприятием и не допустить скупку ценных бумаг внешними инвесторами. Это обеспечивается посредством:

- введения ограничений для доступа сторонних инвесторов к информации об эмиссии;

- создания привилегированных условий приобретения ценных бумаг для отдельных категорий инвесторов.

Эти злоупотребления ущемляют права и законные интересы потенциальных инвесторов, ограничивают конкуренцию.

В целях предупреждения подобных нарушений законодательством предусмотрен порядок, в соответствии с которым:

- в случае открытой (публичной) эмиссии, требующей регистрации проспекта эмиссии, эмитент обязан обеспечить доступ к информации, содержащейся в проспекте эмиссии, и опубликовать уведомление о порядке раскрытия информации в периодическом печатном издании с тиражом не менее 50 тысяч экземпляров;
- эмитент, а также профессиональные участники рынка ценных бумаг, осуществляющие размещение эмиссионных ценных бумаг, обязаны обеспечить любым потенциальным владельцам возможность доступа к раскрываемой информации до приобретения ценных бумаг;
- в тех случаях, когда хотя бы один выпуск эмиссионных ценных бумаг эмитента сопровождался регистрацией проспекта эмиссии, эмитент обязан раскрыть информацию о своих ценных бумагах и своей финансово-хозяйственной деятельности в форме ежеквартального отчета и сообщения о существенных фактах, затрагивающих финансово - хозяйственную деятельность эмитента.

Запрещается при публичном размещении или обращении выпуска эмиссионных ценных бумаг закладывать преимущество при приобретении ценных бумаг одним потенциальным владельцам перед другими.

Вместе с тем, несмотря на запрет подобной дискриминации потенциальных владельцев ценных бумаг указанные злоупотребления получили распространение. Одним из типичных способов достижения этой цели эмитентом является привлечение для размещения ценных бумаг андеррайтера, являющегося аффилированным лицом. Андеррайтер, действуя в интересах эмитента, способен нанести ущерб потенциальным инвесторам.

Среди причин подобных злоупотреблений следует отметить:

а) отсутствие правового механизма обеспечения реальной независимости андеррайтера;

б) отсутствие лицензирования андеррайтинга как самостоятельного вида профессиональной деятельности на рынке ценных бумаг;

в) отсутствие законодательных ограничений на совмещение андеррайтинга с другими видами профессиональной деятельности на рынке ценных бумаг;

г) отсутствие законодательных ограничений на размещение ценных бумаг самим эмитентом;

д) возможность осуществления андеррайтинга аффилированными с эмитентом структурами.

Принятие эмитентом решения о предоставлении к регистрации и регистрацией уполномоченным государственным органом отчета об итогах выпуска эмиссионных ценных бумаг с заведомо недостоверной информацией, например, о фактической цене размещения ценных бумаг, количестве размещенных ценных бумаг, об общем объеме поступлений денежных средств за размещенные ценные бумаги и т.п.

Правовая защита участников рынка ценных бумаг на этапе эмиссии осуществляется посредством введения ответственности за злоупотребления при эмиссии. Ответственность предусмотрена за следующие деяния:

- внесение в проспект эмиссии ценных бумаг заведомо недостоверной информации;
- утверждение проспекта эмиссии, содержащего заведомо недостоверную информацию;
- утверждение заведомо недостоверных результатов эмиссии, если эти деяния повлекли причинение крупного ущерба

6.4.2 Злоупотребления в процессе регистраторской деятельности (деятельности по ведению реестра владельцев эмиссионных ценных бумаг)

Реестр владельцев ценных бумаг представляет собой список зарегистрированных владельцев с указанием количества, номинальной стоимости и категории принадлежащих им именных ценных бумаг, составленный по состоянию на любую установленную дату и позволяющий идентифицировать этих владельцев, количество и категорию принадлежащих им ценных бумаг.

Среди злоупотреблений, характерных для регистраторской деятельности можно выделить:

а) хищение ценных бумаг;

б) неправомерное использование регистратором конфиденциальной информации;

в) оказание давления на владельцев ценных бумаг;

г) злоупотребления эмитента, выполняющего функции трансфер-агента;

д) незаконный отказ от внесения записи в систему ведения реестра;

е) уклонение от внесения такой записи;

ж) внесение в реестр недостоверных сведений;

з) нарушение сроков выдачи выписки из указанного реестра;

и) невыполнение или ненадлежащее выполнение лицом, осуществляющим ведение указанного реестра, иных законных требований владельца ценных бумаг, или лица, действующего от его имени, или номинального держателя ценных бумаг.

Рассмотрим некоторые типичные злоупотребления более подробно.

Хищение акций посредством подложного передаточного распоряжения относится к числу классических злоупотреблений в процессе регистраторской деятельности. Различают две разновидности подобного хищения: совершаемые сторонними лицами и в результате внутреннего сговора персонала.

В первом случае злоумышленник подделывает доверенность от имени компании - собственника акций о том, что компания продает свои акции другому инвестору. При этом он предъявляет передаточное распоряжение с фальшивой подписью. Регистратор, в соответствии с нормативными актами ФКЦБ имеет право потребовать от компании - продавца только передаточное распоряжение. Оператор компании - регистратора сверяет подпись на передаточном распоряжении с имеющимся у него образцом подписи управомоченного лица. Регистратор переводит бумаги на мошенническую компанию, как правило фирму-однодневку, которая переводит бумаги на третью компанию, являющуюся добросовестным приобретателем. Затем мошенническая компания ликвидируется, исключается из реестров государственной регистрации компаний.

Во втором случае преступление совершается злоумышленниками из числа персонала, имеющего доступ к внутренней информации.

Злоупотребления регистратора, связанные с неправомерным использованием конфиденциальной информации могут принимать различную форму:

1. Предоставление эмитенту конфиденциальной информации о лицах, получивших выписки из реестра для продажи акций. Непосредственный мотив данных действий - обеспечить концентрацию власти в руках менеджмента предприятия и воспрепятствовать перераспределению контрольного пакета акций в собственность сторонних инвесторов. Получение конфиденциальной информации о сделках по акциям, осуществленных акционерами - работниками предприятия позволяет использовать ее для оказания давления на них с целью недопущения неконтролируемой администрацией реализации акций.

2. Использование регистратором конфиденциальной информации при осуществлении операций с ценными бумагами. Проблема регулирования доступа эмитента к конфиденциальной информации реестра, ведение которого осуществляет независимый регистратор, в законодательстве даже не обозначена.

3. Содействие отдельным акционерам и администрации эмитента в установлении контроля над предприятием посредством использования незаконных методов. Данные действия были характерны для периода перераспределения собственности в отношении акционеров - членов трудового коллектива предприятия-эмитента. Например, администрация предприятия может оказывать давление на работников, распространять информацию о перспективах предприятия, в то время как регистратор обеспечивает скупку ценных бумаг по заниженному курсу в пользу администрации.

6.4.3 Злоупотребления эмитента, выполняющего функции трансфер-агента.

Трансфер-агентом является юридическое лицо, являющееся агентом регистратора и выполняющее функции по сбору информации для внесения изменений в реестр, передаче этой информации регистратору, а также по оформлению и выдаче документов, удостоверяющих право собственности на ценные бумаги. Трансфер-агент принимает документы, предоставляемые зарегистрированными лицами для внесения изменений в реестр, и пересылает их регистратору.

Выполнение эмитентами функций трансфер-агента не противоречит действующему законодательству. Вред интересам акционеров может быть нанесен посредством внесения в реестр недостоверных данных и сообщении реестродержателю искаженной информации. Основной мотив связан с удержанием контроля над предприятием.

Указанные действия совершаются, как правило в условиях зависимости регистратора от эмитента и имеют целью воспрепятствовать переходу прав собственности на ценные бумаги к сторонним инвесторам.

6.4.4 Злоупотребления в процессе депозитарной деятельности.

Депозитарной деятельностью признается оказание услуг по хранению сертификатов ценных бумаг, их учету и переходу прав на ценные бумаги.

Криминогенным фактором является зависимость депозитария от регистратора, связанного с эмитентом общими интересами. Ущерб, наносимый интересам

владельцев ценных бумаг - депонентов состоит в передаче конфиденциальной информации эмитенту. Причем, если регистратор может не владеть информацией о реальных владельцах ценных бумаг, особенно если в системе ведения реестра депозитарий представлен как номинальный держатель, то зависимый депозитарий является важным источником информации для эмитента.

Довольно распространенным явлением в данной сфере является сбыт фиктивных ценных бумаг. Данное злоупотребление осуществляется посредством незаконного использования компьютерных технологий осуществления депозитарных операций. Оно совершается по следующей типичной схеме.

Выбирается лицевой счет, на который с помощью стороннего программного обеспечения производится фиктивное списание акций с большой группы счетов.

Для обеспечения баланса системы расчетов сторонним программным обеспечением создается фиктивная запись, никому не принадлежащая, с отрицательным количеством акций, равным сумме акций всех накопительных счетов. В итоге на счете, реально содержащем иное количество акций, создается значительный пакет акций, который с точки зрения системы расчетов имел легальный статус.

Владелец накопительного счета (иногда с фиктивной доверенностью) оформляет в депозитарии “легальный перевод” со своего счета на счет другого регионального депозитария. Сотрудники депозитария оформляют передачу. Таким образом, происходит легализация фиктивных акций.

На накопительном счете восстанавливается исходное количество акций, и уничтожаются все следы воздействия стороннего программного обеспечения.

Другими распространенными преступлениями в процессе депозитарной деятельности являются хищения депонированных ценных бумаг.

6.5 Недобросовестная торговля

Недобросовестная торговля - это совершение операций на рынке ценных бумаг, имеющие либо способные вызвать негативные последствия, как для отдельных участников, так и для рынка в целом.

Недобросовестная торговля проявляется в:

а) манипулирование ценами;

б) торговле с использованием инсайдерской информации (злоупотреблении инсайдерской информацией);

в) спекуляции на рынке ценных бумаг;

г) нарушение брокерами (дилерами) интересов своих клиентов.

Для обеспечения экономической безопасности на рынке ценных бумаг большое внимание необходимо уделять манипуляциям на рынке.

6.5.1 Манипулированием рынком

Под «**манипулированием рынком**» подразумеваются любые действия, направленные на создание ложных ценовых ориентиров. Под это определение попадают более 20 различных операций с ценными бумагами. Наиболее распространенные среди них:

а) заключение большого количества сделок с акциями по котировкам, отличных от средних по рынку;

б) искусственное завышение объемов торгов путем покупки и моментальной продажи акций без перерегистрации прав собственности;

в) сосредоточение большого количества акций одного эмитента у одной или группы компаний, в результате которого мелкие спекулянты вынуждены выкупать эти акции для закрытия позиций по завышенной цене;

г) неоправданное повышение (понижение) цен с последующей продажей (скупкой) ценных бумаг. Манипулятор, называясь осведомленным лицом и распространяя 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. Данный прием используется в условиях отсутствия или недостатка информации о компании, ценные бумаги которой торгуются на рынке. Данная схема может применяться и в обратном варианте с целью игры на понижение котировок акций того или иного эмитента.

Так, например, в 2002 году Марк Джакоб распространил от имени компании Emulex сообщение для печати, в котором утверждалось, что компания пересмотрела свои финансовые показатели за последний отчетный период и пришла к выводу о наличии убытков вместо ранее заявленной прибыли. В результате, цена акций компании Emulex упала с $100 до $43 за акцию. Торговля акциями компании была приостановлена после объявления о недостоверности опубликованных сведений. Однако потери инвесторов за время торгов составили около 2 млрд. долл. Как было установлено, сам Марк Джакоб приобрел 3500 акций Emulex после значительного падения их стоимости по цене около $50 за акцию, а затем реализовал их после объявления о ложном характере распространенных сведений по цене $105 за акцию. В результате этой операции преступник получил прибыль в размере 186 814 долл.

6.5.2 Торговля с использованием инсайдерской информации

Большое влияние на рыночную манипуляцию оказывают инсайдеры, которые в своей торговле используют информацию, неизвестную рядовому инвестору. Торговля с использованием информации, которая доступна не всем участникам рынка (инсайдерская информация), наряду с мошенническими операциями относится к числу самых серьезных нарушений на финансовом рынке.

Инсайдеры – это лица, располагающие служебной информацией. По российскому законодательству (ст. 32 ФЗ «О рынке ценных бумаг») к ним относят:

1. Членов органов управления эмитента или профессионального участника рынка ценных бумаг, связанного с этим эмитентом договором;

2. Аудиторов эмитента или профессионального участника рынка ценных бумаг, связанного с этим эмитентом договором;

3. Служащих государственных органов, имеющих в силу контрольных, надзорных и иных полномочий доступ к указанной информации.

В нормативных документах некоторых стран к категории инсайдеров также относят:

- крупных акционеров, владеющих 10% и более акций эмитента (США, Япония);
- членов органов управления компании, осуществляющей поглощение другой компании (Япония);

- близких родственников всех перечисленных лиц (Великобритания);
- служащих компании, имеющих доступ к служебной информации;
- лиц, получающих информацию от всех вышеперечисленных лиц, так называемых «вторичных» инсайдеров (Япония, Великобритания).

Последняя категория лиц специально выделяется в законах рядя стран, где инсайдеры делятся на «первичных» и «вторичных».

Кроме того, к инсайдерам относят чиновников и лиц, связанных с одной компанией, но совершающих сделки с ценными бумаги другой компании и имеющих о последней сведения в силу своего положения в первой компании, если эти сведения носят характер неопубликованной информации, которая может оказать влияние на цены. К лицам, связанным с компанией, относят:

1. Директора данной компании или связанной с ней компании;
2. Руководители подразделений и сотрудники данной компании или связанной с ней компании;
3. Лица, которые в силу своего профессионального положения имеют связи с данной компанией.

Инсайдеры, используя известную только им информацию о том или ином эмитенте, принимают решения о покупке (продажи) определенных ценных бумаг, что довольно часто приводит к резкому повышению (понижению) их котировок. Об этом было сказано выше. Разница состоит лишь в том, что они заключают сделки, основываясь на достоверной информации, которая становится им известна намного раньше, чем другим участникам рынка. Соответственно они реагируют на эту информацию быстрее и заключают сделки на более выгодных условиях.

Рассмотрим, использование инсайдерской информации на примере присвоения в прошлом году России инвестиционного рейтинга. Понятно, что эта информация сначала стала известна очень узкому кругу лиц (инсайдерам). Так как это положительная новость, то инсайдеры начали скупку акций на российском фондовом рынке. В результате объемы торгов и цены акций на рынке начали постепенно расти. Далее эта новость стала известна значительному числу трейдеров и спекулянтам. Они тоже начали скупку акций. В результате цены на акции стали расти более быстрыми темпами, объемы торгов по-прежнему оставались на высоком уровне. В середине дня цены, казалось, достигли своего пика, и начали корректировать вниз (коррекция в среднем составила 2-3%). Инсайдеры во время этой коррекции зафиксировали прибыли и вышли в деньги. Когда о присвоении рейтинга узнали все остальные инвесторы, они также начали скупать акции. Рост цен возобновился.

Большое внимание необходимо уделять также и спекулятивным играм на рынке ценных бумаг.

6.5.3 Спекуляция на рынке ценных бумаг

Спекуляция на рынке ценных бумаг - торговля ценными бумагами с целью получения прибыли за счет разницы их курсов. В условиях срочной биржевой торговли спекуляция базируется на разнице курсов фьючерсных контрактов.

Спекулятивная деятельность на рынке ценных бумаг выполняет важную позитивную функцию, которая состоит в перенесении риска с тех участников рынка, которые не желают его принимать (хеджеров), на тех участников, которые стремятся к принятию риска (спекулянтов). Кроме того, спекулянты обеспечивают

такое важное качество рынка как его ликвидность, создавая условия для заключения в кратчайшие сроки сделок по купле и продаже фондовых инструментов. Однако, создавая возможности для снижения риска ценовых колебаний для хеджеров, деятельность спекулянтов может принимать общественно нежелательные формы, связанные, как правило, с целенаправленным воздействием на цены фондовых инструментов и получением прибыли посредством незаконного использования при заключении сделок инсайдерской (служебной) информации, а также манипулирование ценами.

В качестве примера недобросовестной торговли можно рассмотреть события, происходившие вокруг крупной нефтяной компании «ЮКОС» летом этого года. Были дни, когда цены на акции этой компании за день поднимались (опускались) на 10-20%. В результате резкого повышения (понижения) цен на бирже не раз приостанавливались торги этими акциями.

Итак, летом почти каждый день выходили то положительные, то отрицательные новости, касающиеся компании «ЮКОС», что незамедлительно отражалось на котировках ценных бумаг компании. Кто, бесспорно, выиграл от чехарды вокруг "ЮКОСа", так это биржевые спекулянты. Для них, при хорошей информированности и умелой работе, ежедневные проходы акций по 10-20% – золотое дно. За что они должны благодарить «ньюсмейкеров» из МНС и Минюста.

Рассмотрим период с 17.06.04г. по 05.08.04г. На рисунке 6.2 изображен дневной график акций «ЮКОСа». Черная свеча означает падение цены акции в течение день, белая – ее повышение.

Рисунок 6.2 - Дневной график акций «ЮКОСа»

С апреля 2004 года цены на акции Юкоса падают в результате налоговых претензий к этой компании. За 2 месяца акции подешевели на 70%. В отдельные дня котировки акций понижались (повышались) в течение дня на несколько процентов. Так впервые с апреля значительное повышение котировок наблюдалось 17 июня в результате заявления президента России В. Путина в Ташкенте в рамках саммита Шанхайской организации сотрудничества о том, что власти не заинтересованы в банкротстве нефтяной компании «ЮКОС». Более того, правительство должно всячески постараться и не обрушить акции. Биржевым игрокам хватило полчаса на осознание значимости момента: в РТС и на ММВБ ценные бумаги НК "ЮКОС" взлетели на 20 и 30% соответственно. Ближе к вечеру, в соответствии с регламентом бирж, пришлось приостановить торги на час, поскольку ценные бумаги этой компании выросли в РТС к 17:00 на 34,19% до $8,32 за акцию, а в фондовой секции ММВБ к 17:10 они поднялись 34,93% до 255 руб.

Эксперты отмечают, что на рынке существуют целые группы "скромных околовластных брокеров", которые на перепадах курса акций "ЮКОСа" делали, делают и будут еще какое-то время делать неплохие деньги. В результате этого страдают неопытные инвесторы, которые, испугавшись падения акций, начинают избавляться от них, даже неся при этом убытки. Защиты от этих действий у регуляторов нет - запрет на проведение торгов "ЮКОСа" нарушил бы права инвесторов: "Может, кто-то хочет продать акции по любой цене. Максимум, что возможно при резком падении акций компании, - это временная приостановка торгов».

6.5.4 Нарушение брокерами (дилерами) интересов своих клиентов

Брокерской является деятельность по совершению гражданско-правовых сделок с ценными бумагами в качестве поверенного или комиссионера, действующего на основании договора поручения или комиссии, а также доверенности на совершение таких сделок при отсутствии указаний на полномочия поверенного или комиссионера в договоре. Таким образом, брокер действует на рынке ценных бумаг от имени и за счет клиента, получая доход в форме комиссионных.

Дилерской является деятельность по совершению сделок купли - продажи ценных бумаг от своего имени и за свой счет путем публичного объявления цен покупки и/или продажи определенных ценных бумаг с обязательством покупки и/или продажи этих ценных бумаг по объявленным ценам. Дилер осуществляет сделки купли-продажи от своего имени и за свой счет. Источником его дохода является разница курсовой стоимости покупаемых и продаваемых ценных бумаг.

Деятельность по **управлению ценными бумагами** - осуществление юридическим лицом или индивидуальным предпринимателем от своего имени за вознаграждение в течение определенного срока доверительного управления переданными ему во владение и принадлежащими другому лицу в интересах этого лица или указанных этим лицом третьих лиц: ценными бумагами; денежными средствами, предназначенными для инвестирования в ценные бумаги; денежными средствами и ценными бумагами, получаемыми в процессе управления ценными бумагами.

Часто, особенно на американском рынке, встречаются мошенничества со стороны брокеров.

Конкретных схем и моделей подобных злоупотреблений достаточно много. Рассмотрим некоторые из них:

1. Переложение риска операций с ценными бумагами на клиента.
2. Присвоение части дохода клиента от операций с принадлежащими ему ценными бумагами.
3. Хищение ценных бумаг под прикрытием брокерской деятельности.
4. Приобретение брокерскими фирмами для клиентов заведомо фальшивых ценных бумаг.
5. Мошенническое присвоение ценных бумаг либо проведение сделок с ценными бумагами в ущерб клиенту со стороны иностранной компании, не имеющего лицензии на совершение операций с ценными бумагами российских эмитентов.
6. Злоупотребления со средствами клиентов путем использования оффшорных схем работы с ценными бумагами.

Переложение риска операций с ценными бумагами на клиента.

Недобросовестный брокер, пользуясь неосведомленностью клиента о характере фактически совершаемых операций с его средствами, в случае неудачной сделки по покупке ценных бумаг, легко может переложить риск на клиента, “убедив” его в необходимости их покупки. В результате в портфеле у клиента могут оказаться бросовые малоликвидные и дорогие ценные бумаги.

Частным случаем является введение в заблуждение инвестора при операциях по формированию крупных пакетов неликвидных акций. Они скупаются инвестиционными институтами с целью последующей перепродажи по значительно более высокой цене стратегическим инвесторам, намеревающимися приобрести контроль над предприятием. В случае успеха операции компания присваивает основную долю прибыли, делясь ее незначительной частью (как правило, в 4-5 раз меньшей) с инвесторами, средства которых и использовались для реализации схемы. При отсутствии покупателя неликвидные ценные бумаги распределяются вместе с убытками по инвестиционным портфелям клиентов. В случае же удачной продажи основную часть прибыли получает инвестиционная компания.

Данные злоупотребления характерны также для деятельности сотрудников коммерческих банков, являющихся дилерами на рынке ценных бумаг. При высокой ликвидности и емкости рынка ситуация на нем меняется очень динамично и разброс доходности по операциям очень велик. В этой ситуации дилер может использовать в игре на рынке свои собственные средства, относя все низкодоходные и неудачные сделки на счет банка, оформляя в то же время наиболее эффективные сделки как проведенные за счет собственных средств. При этом контролировать деятельность сотрудников службы дилинга крайне затруднительно. Они являются своеобразной кастой со своими неписаными законами, обладающими значительными полномочиями, доступом к конфиденциальной информации и значительным доверием в кругу профессионалов. Потенциальных возможностей совершить злоупотребление у дилера больше, чем у иных сотрудников финансовых учреждений.

Присвоение части дохода клиента от операций с принадлежащими ему ценными бумагами.

Мотивами подобного поведения дилера может быть отсутствие заинтересованности в дальнейшем сотрудничестве с конкретным инвестором,

предоставляющим в доверительное управление слишком незначительные суммы, или вообще дальнейших поступлений от клиента не ожидается. Дилер всегда может свести доход клиента от операций с ценными бумагами к необходимому минимуму и не осуществлять никаких дополнительных выплат клиенту.

Недобросовестные дилеры могут в договоре о доверительном размещении средств клиента сделать оговорку о возможности использования денежных средств клиента в других секторах финансового рынка. Клиенту данная оговорка объясняется с позиций необходимости ухода банка-дилера с помощью подобного размещения средств от резервирования. Таким образом, у дилера в случае, если он уже достиг в результате операций со средствами клиента необходимого минимума, есть легальная возможность сбыть клиентские облигации и до наступления срока платежа вполне законно “прокручивать” деньги клиента в своих собственных интересах.

Хищение ценных бумаг под прикрытием брокерской деятельности.

Мошенники, выступая в роли брокеров, принимают к продаже пакты корпоративных ценных бумаг. В дальнейшем вырученные от их продажи деньги переводятся ими на счета подставных фирм и присваиваются. Такие действия имели место в отношении пакетов акций РАО «ЕЭС России», РАО «Газпром» и АО «НК ЛУКойл».

Мошенническое присвоение ценных бумаг либо проведение сделок с ценными бумагами в ущерб клиенту со стороны иностранной компании, не имеющего лицензии на совершение операций с ценными бумагами российских эмитентов.

В результате контракты с данной фирмой и совершенные ей сделки с ценными бумагами являются недействительными. Кроме того, зачастую инвестор не имеет возможности выяснить историю своих операций с ценными бумагами и получить их. В этой схеме иностранная компания также может выполнять и функции депозитария.

Злоупотребления со средствами клиентов путем использования оффшорных схем работы с ценными бумагами.

В этой схеме средства клиента через оффшорную компанию переводятся на счета инвестиционной компании, которая получает возможность практически бесконтрольно распоряжаться средствами клиента зачастую далеко не в его интересах. С инвестиционной компанией заключается депозитарный и брокерский договоры. Заключение депозитарного договора позволяет не регистрировать акции на имя клиента. Согласно брокерскому договору деньги клиентов для операций с акциями хранятся на счетах самой компании. Таким образом, средства клиента юридически не отделены от средств компании, а портфели клиентов существуют лишь формально. Фактически, используя депозитарный и брокерский договоры, инвестиционная компания получает возможность, не отделяя своих средств от средств клиента, проводить рисковые операции, перекладывая риск убытков на клиента и гарантированно присваивая прибыль.

Рассмотрим некоторые случаи мошенничества со стороны брокеров на конкретных примерах.

20 ноября 2002 года агенты ФБР ворвались в южную башню Всемирного финансового центра в США. А спустя несколько минут людей в дорогих костюмах с наручниками на руках, одного за другим, начали выводить и сажать в «воронки».

Вскоре всем арестованным предъявили целый список обвинений – отмывание денег, мошенничество, вымогательство, злостное банкротство, угрозы, нарушение законодательства об огнестрельном оружии, дача взяток и прочее. Всего было задержано 28 человек.

Жертвами злоумышленников стали свыше тысячи физических и юридических лиц, начиная от мелких инвесторов и кончая крупными банками. Именно жалобы мелких инвесторов на нечистоплотность обслуживающих их брокеров позволили ФБР выйти на след преступников.

Ущерб исчислялся миллионами долларов. Обвинения были предъявлены трейдерам и брокерам крупнейших игроков валютного рыка США – американских банков JP Morgan, UBS Warburg, Dresdner Kleinwort Benson, французского Societe Generale и израильского Discount Bank. В махинациях были замешаны, по меньшей мере, четыре крупные фирмы. Среди арестованных были трое сотрудников компании ICAP и семеро – из Madison Deane and Associates: три партнера, три вице-президента и брокер.

В другом деле «США против Вито Наполетано и других» престали 8 обвиняемых. С 2000 по 2002 год они обманули несколько сотен мелких инвесторов. Собранные средства уходили на личные нужды обвиняемых. Чтобы вкладчики были уверены в прибыльности вложений, мошенники печатали им фальшивые выписки со счетов. Обвиняемые создали три фирмы для привлечения денег инвесторов и обманули последних почти на 1 миллион долл.

Самым громким делом стало дело «США против Пола Балласа и других». По нему проходила группа из 20 обвиняемых, которые занимались махинациями на валютных рынках. Сами преступники называли это игрой «очки за наличные», которая предполагала заведомо убыточные для клиента операции, а затем «откат черным налом» партнеру. Схема на протяжении многих лет действовала безошибочно. Продавцы валюты из крупных финансовых учреждений (JP Morgan, Dresdner Bank, UBS, Societe Generale и Discount Bank) проводили заведомо невыгодные для своих банков и клиентов операции на мировом валютном рынке. Межбанковские брокеры оказывали посреднические услуги при покупке или продаже валюты от имени банков. А так называемый контрагент – американская фирма Itrade Currency – обеспечивала тот самый «откат», используя невыгодный курс покупки и перечисляя разницу на специальные счета, открытые для обналичивания незаконных доходов.

6.6 Обеспечение безопасности рынка ценных бумаг

С развитием рыка ценных бумаг значительно возрастает его уязвимость от внешних воздействий. Российский рынок ценных бумаг остается незащищенным от различного рода преступных посягательств. Поэтому необходимо исследовать проблемы безопасности рынка, вырабатывать концептуальные подходы и практические меры по ее обеспечению на основе анализа зарубежного и отечественного опыта.

Значительная роль по обеспечению безопасности на рынке ценных бумаг отводится государству. Однако в концепции развития рынка ценных бумаг России акцент делается на принцип саморегулирования и формирования в перспективе саморегулирующей системы, что не совсем верно даже для рыка корпоративных ценных бумаг. В развитых странах рынок формировался десятки лет и постепенно

сложилась стройная и надежная система его безопасности. Так, система регулирования и обеспечения безопасности рынка ценных бумаг США начала активно создаваться после финансового кризиса в 1933-1934 г.г., когда был принят ряд законов. В течение длительного времени она совершенствовалась и в последнее время приобрела в большей степени саморегулируемый характер. Речь идет о рынке корпоративных и производных ценных бумаг. Рынок государственных долговых обязательств регулируется и обеспечивается государством и его правоохранительными органами.

В период развития нашего рынка необходимо повышать роль государства и его органов в области регулирования и обеспечения безопасности. Государство должно формировать законодательную и нормативную базу функционирования рынка, организовывать систему правоприменения и выполнять регулирующую функцию.

Реформирование нормативной и правовой базы рынка ценных бумаг необходимо осуществлять, используя следующие основные принципы:

1. Декларирование политики в области развития рынка ценных бумаг, совершенствования его нормативной и правовой базы в целях информирования его субъектов о планируемых изменениях правового режима;
2. Распределение полномочий по регулированию рынка между РФ и субъектами РФ, а также различными органами исполнительной власти;
3. Усиление государственного контроля за деятельностью участников рынка, повышение роли и ответственности регулирующих и правоохранительных органов, и в первую очередь Федеральной службы по финансовым рынкам (ФСФР);
4. Организация системы налогообложения операций с ценными бумагами, имеющей не фискальный, а стимулирующий характер;
5. Преимущественная и всесторонняя защита законных прав и интересов инвесторов, пресечение незаконной деятельности на рынке, повышение ответственности профессиональных участников рынка и эмитентов за результаты своей деятельности;
6. Поддержка государством добровольного страхования рисков профессиональными участниками рынка ценных бумаг. При этом государство не должно брать на себя обязательства по компенсации незастрахованных рисков;
7. Обеспечение инвесторов полной и достоверной информацией о ценных бумагах и их эмитентах, развитие вневедомственного и общественного контроля за достоверностью информации;
8. Усиление контроля за соблюдение условий лицензирования при осуществлении профессиональной деятельности на рынке, повышение требований к лицензированию профессиональных участников рынка, обеспечивающих высокий уровень их квалификации, достаточность собственных средств, поддержание высоких стандартов добросовестности и открытость при осуществлении ими профессиональной деятельности;
9. Создание равных условий и обеспечение конкуренции при осуществлении предпринимательской деятельности на рынке ценных бумаг.

Повышенное внимание должны привлечь такие правонарушения, как мошенничество, манипуляция с ценными бумагами, которые в настоящее время составляют значительную долю. Им необходимо дать четкую квалификацию с учетом особенностей российского рынка.

Особая роль в регулировании рынка ценных бумаг возлагается на ФСФР. Для активизации государственного регулирования фондового рынка должен быть повышен ее статус, ФСФР должна быть наделена также соответствующими полномочиями. В ней целесообразно создать подразделения безопасности (по аналогии с подобными комиссиями в других странах).

Одним из приоритетных направлений государственного регулирования должно стать продолжение работы по раскрытию информации и повышению уровня прозрачности рынка ценных бумаг.

При поддержке заинтересованных федеральных органов исполнительной власти ФСФР осуществляет формирование системы информационного и телекоммуникационного обеспечения своей деятельности. Эта система должна обеспечить оперативный обмен базами данных по лицензированию и надзору за деятельностью профессиональных участников фондового рынка между подразделениями ФСФР, других федеральных органов исполнительной власти и включать в себя как закрытую часть (служебную информацию, связанную с вопросами лицензирования и надзора), так и открытую, доступную всем заинтересованным сторонам.

Важнейшей политической и экономической проблемой России является привлечение иностранных инвестиций и защита инвесторов. В этих целях необходимо дальнейшее совершенствование законодательства и скоординированные меры правоохранительных органов по обеспечению безопасности инвесторов.

Без наведения элементарного порядка в сфере вексельного обращения и принятия дополнительных мер по обеспечению безопасности этого сегмента рынка ценных бумаг невозможно решить финансовые и экономические проблемы страны. Необходимо завершить создание единого информационного массива сферы обращения векселей.

Для ограничения возможностей совершения мошеннический действий по купле-продаже векселей и других ценных бумаг специалисты рекомендуют выполнять следующие требования:

1. Для разных документов использовать разные бланки и печати, образцы которых должны быть только в тех организациях, которые работают с банком;
2. Резко ограничить доступ сотрудников банка, не имеющих к этому отношения, ко всем видам бланков, образцам подписей руководителей и печатей банка;
3. Ввести систему защиты самих бланков, подделка которых с использованием компьютерной техники невозможна (в первую очередь это относится к использованию специальных сортов бумаги и водяных знаков);
4. Не допускать служащих (а тем более представителей других организаций) к составлению и печати документов, к которым по роду работы они отношения не имеют;
5. Использовать для пересылки важных финансовых документов защищенные каналы связи и защищать передаваемую информацию;
6. Четко прописывать в договорах систему приема-передачи ценных бумаг и оговаривать порядок перепроверки документов, используя как минимум двойную систему проверки: предоставление письменного документа и устное распоряжение руководителей, имеющих соответствующие права;

7. Тщательно проверять контрагентов по сделкам, используя все доступные для этого средства (желательно при этом копирование документов, удостоверяющих личность).

Кроме мероприятий по проверке конкретной сделки, в масштабе города (региона) целесообразно:

1. Создавать банки данных об участниках вексельных сделок (их деловой активности, платежеспособности, наличии просроченных долговых обязательств, лицах, замеченных в совершении сомнительных сделок и мошенничеств, типичных схемах-предложений, предлагаемых мошенниками);

2. Систематически публиковать информацию о рейтинге векселедателей и акцептантов, разработав методику оценки их финансового состояния (такая работа уже проводится рядом банков и других коммерческих структур, работающих на рынке ценных бумаг).

Цель таких мероприятий - повышение прозрачности вексельного рынка и значительное уменьшение числа злоупотреблений с использованием векселей, и, как следствие, стабилизация и декриминализация этого рынка.

Таким образом, усиление роли государства в формировании, регулировании и обеспечении безопасности отечественного рынка ценных бумаг является жизненно важной необходимостью и требует принятия руководством страны соответствующих мер.

Вопросы для повторения темы:

1. Дайте определение ценной бумаге.
2. Раскройте основной состав правонарушений на рынке ценных бумаг.
3. Какое информационное правонарушение на рынке ценных бумаг характеризуется повышенной общественной опасностью и почему?
4. Перечислите основные виды подделок ценных бумаг.
5. Перечислите основные дефекты формы в векселях.
6. Действительны ли документы, в которых вместо собственноручной подписи соответствующего руководителя наносится его факсимиле?
7. Какую опасность таят в себе «серые» схемы расчета векселями?
8. Раскройте механизм схемы искусственного раздувания спроса.
9. Что Вы понимаете под «бронзовым векселем»?
10. Почему ряд финансистов считают, что производные финансовые инструменты являются оружием массового поражения и несут катастрофические риски для мировой экономики.
11. Какие этапы включает процесс эмиссионной деятельности?
12. Чем обусловлено создание преимущественных условий приобретения ценных бумаг для отдельных категорий потенциальных инвесторов?
13. Перечислите основные злоупотребления, характерные для регистраторской деятельности.
14. Какие формы могут принимать злоупотребления регистратора?
15. Дайте определение недобросовестной торговле. В чем она может проявляться на рынке ценных бумаг?
16. Может ли спекуляция выполнять позитивную функцию на РЦБ?
17. Какие действия по купле-продаже векселей рекомендуют выполнять специалисты для ограничения возможностей мошеннических действий?

Литература:

1. Гордеев А. «Аналитики играют по новым правилам» // Валютный спекулянт. 2003. №12 (50). с. 12-13

2. Жилин И., Масич А. «Экспертиза ценных бумаг – средство снижения потерь от подделок» // РЦБ. 2000. №2 (161). с. 39-50

3. Карабаналов С.С. «Компьютерное мошенничество при торговле ценными бумагами» // Финансовый бизнес. 2002. №6. с. 61-63

4. Недомолкина Л. «Слово – не воробей» // Валютный спекулянт. 2003. №8 (46). с. 7

5. Плисецкий Д.Е. «Финансовая глобализация и национальная экономическая безопасность» // Финансы и кредит. 2004. №4 с. 90

6. Потапов А. «Наручники для брокеров» // Валютный спекулянт. 2003. №12 (50) с. 64-65

7. Потехин В. «Обман по-русски» // Валютный спекулянт. 2003. №8 (46). с. 33

Глава 7. Экономическая безопасность в кредитно-банковской сфере

Ключевые понятия:

Хозяйственное положение
Лжепредпринимательство
фиктивных предприятий
Финансовое состояние
Льготные условия кредитования
Государственный целевой кредит
правовыми критериями
Финансовые критерии
нефинансовых факторах
Залог
Поручительство
Гарантия
Страхование ответственность
Цессия
обеспечительный вексель
Система физической защиты
Система охранных мер
Система регулирования доступа
Система сохранности ценностей

7.1 Общие положения

Обобщая точки зрения, имеющиеся в современной литературе, можно сказать, что обеспечение экономической безопасности банковской деятельности - это процесс достижения состояния защищенности экономических интересов банка, проявляющихся в ходе реализации его уставных целей и задач, и заключается в создании благоприятных условий для реализации всех предусмотренных уставом видов банковской деятельности. Уровень обеспечения экономической безопасности банка определяется общепринятыми критериями его надежности, а также другими показателями, характеризующими его способность противостоять различным негативным явлениям.

Сущность экономической безопасности в банковской системе состоит в обеспечении состояния наилучшего использования ее ресурсов по предотвращению угроз коммерческим банкам и созданию условий стабильного, эффективного функционирования и максимизации прибыли.

Уровень экономической безопасности банковской деятельности определяется тем, насколько эффективно подразделениям и службам банков удается предотвращать угрозы и устранять ущерб от негативного воздействия на

банковскую систему. Источниками таких воздействий являются сознательные или неосознанные действия конкретных людей, а также банков - конкурентов, органов государственной власти, международных организаций.

Главная цель обеспечения безопасности банковской деятельности заключается в достижении устойчивого и максимально эффективного функционирования коммерческих банков на данный момент времени и с учетом перспективной динамики развития, что достигается при решении следующих задач по обеспечению безопасности банковской деятельности:

а) достижение достаточной финансовой устойчивости, конкурентоспособности и независимости коммерческого банка;

б) защита законных прав и интересов банка и его сотрудников;

в) формирование и поддержание высокого технического и технологического потенциала, противодействие техническому проникновению в преступных целях;

г) своевременная и полная гражданско-правовая и уголовно-правовая защита всех видов банковской деятельности;

д) защита информационной среды коммерческих банков и сведений, составляющих банковскую тайну;

е) сохранность материальных ценностей;

ж) защита сотрудников банка от насильственных посягательств, формирование условий для их безопасной работы;

з) контроль за эффективностью функционирования системы безопасности и ее техническое оснащение.

Организация и функционирование системы безопасности банка должны соответствовать следующим принципам:

1. **Комплексность**:

а) обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;

б) обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования;

в) способность системы к развитию и совершенствованию в соответствии с изменениями условий функционирования банка.

Комплексность достигается:

- обеспечением соответствующего режима и охраны КБ;
- организацией специального делопроизводства с ориентацией на защиту коммерческих секретов и банковской тайны;
- мероприятиями по подбору и расстановке кадров;
- широким использованием технических средств безопасности и защиты информации;
- развернутой информационно-аналитической и детективной деятельностью.

Комплексность реализуется совокупностью правовых, организационных и инженерно-технических мероприятий.

2. **Своевременность. У**преждающий характер мер обеспечения безопасности.

Своевременность предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности на основе анализа и прогнозирование финансовой обстановки, угроз безопасности банка, а также разработку эффективных мер предупреждения посягательств на законные интересы.

3. **Непрерывность.** Считается, что злоумышленники только и ищут возможность, как бы обойти защитные меры, прибегая для этого к легальным и нелегальным методам.

4. **Активность**. Защищать интересы банка необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

5. **Законность**. Предполагает разработку системы безопасности на основе федерального законодательства в области банковской деятельности, информатизации и защиты информации, частной охранной деятельности и других нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

6. **Обоснованность**. Используемые возможности и средства защиты должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

7. **Экономическая целесообразность** и сопоставимость возможного ущерба и затрат на обеспечение безопасности (критерий "эффективность - стоимость"). Во всех случаях стоимость системы безопасности должна быть меньше размера возможного ущерба от любых видов риска.

8. **Специализация**. Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными специалистами службы безопасности банка, его функциональных и обслуживающих подразделений.

9. **Взаимодействие и координация**. Означает осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений и служб, сторонних специализированных организаций в этой области, координации их усилий для достижения поставленных целей, а также сотрудничества с заинтересованными объединениями и взаимодействия с органами государственного управления и правоохранительными органами.

10. **Совершенствование**. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, достигнутого отечественного и зарубежного опыта.

11. **Централизация управления**. Предполагает самостоятельное функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованным управлением деятельностью системы безопасности.

Своевременное выявление внешних и внутренних банковских угроз составляет основу для организации действенного управления процессом обеспечения экономической безопасности банковской деятельности.

Оперативное управление этим процессом состоит в регулярном получении информации о состоянии безопасности в каждом конкретном банке, появлении угроз, а также выявлении их возможного воздействия на банковскую деятельность.

Общие подходы к обеспечению экономической безопасности банковской деятельности представлены на рисунке 7.1.

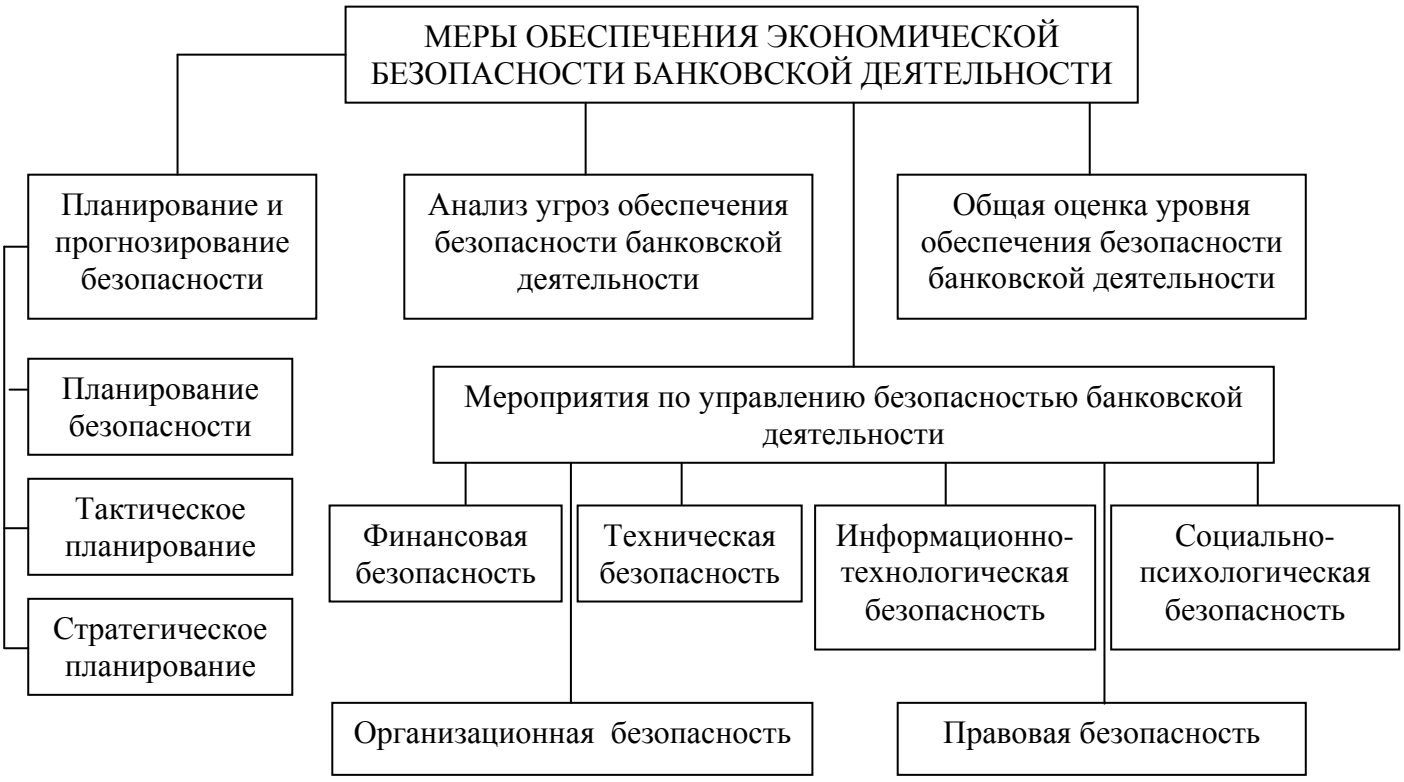

Рисунок 7.1 - Общие подходы к обеспечению экономической безопасности банковской деятельности

Система приведенных мер позволяет обеспечивать устойчивую экономическую безопасность банковской деятельности. Основу этих мероприятий составляет планирование и прогнозирование. Прогнозные оценки находят отражение в стратегическом плане банка, содержащем качественные параметры использования всех имеющихся ресурсов. Для реализации стратегии обеспечения банковской безопасности определяются основные тактические шаги. Наиболее оптимальной представляется разработка нескольких альтернативных сценариев развития ситуации в коммерческом банке и расчета показателей обеспечения экономической безопасности банковской деятельности по каждому из них. После выбора оптимального варианта по результатам расчетов осуществляется составление текущих банковских планов.

Реализация планов обеспечения безопасности банковской деятельности возможна лишь при непосредственном анализе угроз экономической безопасности.

По мнению большинства специалистов, основными составляющими обеспечения экономической безопасности банковской деятельности являются:

- финансовая:
- техническая;
- правовая;
- информационно-технологическая;
- социально-психологическая;
- организационная.

Наиболее важной и сложной является проблема обеспечения финансовой составляющей безопасности коммерческого банка, т.к. в устойчивом, эффективно работающем банке имеются достаточные средства для решения задач по защите информации, охране сотрудников банка, привлечению во все структуры высококвалифицированных специалистов.

С другой стороны, финансовая составляющая - это результирующая всех других составляющих, ее высокий уровень предопределяется успешностью действий по другим составляющим.

Сущность финансовой составляющей безопасности банковской деятельности состоит в обеспечении организационно-управленческих, режимных, технических и профилактических мер, гарантирующих качественную защиту прав и интересов коммерческого банка, рост уставного капитала, повышение ликвидности активов, обеспечение возвратности кредитов, сохранность финансовых и материальных ценностей.

Уровень и интенсивность преступлений в отношении банковских структур свидетельствуют о недостаточной осведомленности служб безопасности о процессах, происходящих как внутри банков, так и в среде их функционирования. Для учета особенностей и тенденций криминального воздействия следует постоянно осуществлять криминологический мониторинг. Следует обратить особое внимание на наиболее распространенные и опасные нарушения закона в кредитной сфере:

- похищения и угрозы похищения сотрудников, членов их семей и близких родственников;
- убийства, сопровождаемые насилием;
- психологический террор, угрозы, запугивание, шантаж, вымогательство;
- нападение с целью завладения денежными средствами, ценностями и документами.

Преступные посягательства в отношении помещений (в том числе и жилых), зданий и персонала проявляются в виде:

- взрывов;
- обстрелов из огнестрельного оружия;
- минирования, в том числе с применением дистанционного управления;
- поджогов;
- нападения, вторжения, захватов, пикетирования, блокирования;
- повреждения входных дверей, решеток, ограждений, витрин, мебели, а также транспортных средств личных и служебных;
- технологических аварий, пожаров.

Цель подобных акций:

- нанесение серьезного морального и материального ущерба;
- срыв на длительное время нормального функционирования;

- вымогательство значительных сумм денег или каких-либо льгот (кредиты, отсрочка или погашение платежей и т.п.) перед лицом террористической угрозы.

В таблице 7.1 приведены основные угрозы финансовым и информационным ресурсам кредитных организаций.

Таблица 7.1 - Угрозы финансовым и информационным ресурсам кредитных организаций

Угрозы финансовым ресурсам проявляются в виде:	• невозврата кредитных ссуд; • мошенничества со счетами и вкладами; • подложных платежных документов и пластиковых карт; • хищения финансовых средств из касс и инкассаторских машин.
Угрозы информационным ресурсам проявляются в виде:	• разглашения конфиденциальной информации; • утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения; • несанкционированного доступа к охраняемым сведениям со стороны конкурентных организаций и преступных формирований.

Осуществление угроз информационным ресурсам может быть произведено:

1) путем неофициального доступа и съема конфиденциальной информации;

2) путем подкупа лиц, работающих в банке или структурах, непосредственно связанных с его деятельностью;

3) путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники с помощью технических средств разведки и съема информации, несанкционированного доступа к информации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения;

4) путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте, на квартирах и дачах;

5) через переговорные процессы между банком и иностранными или отечественными фирмами, используя неосторожное обращение с информацией;

6) через отдельных сотрудников банка, стремящихся заполучить больший, чем их зарплата, доход или имеющих иную корыстную либо личную заинтересованность.

Коммерческие банки являются приоритетными объектами для совершаемых преступными группами посягательств, связанных с их криминальным промыслом, таких, как:

- принуждение должностных лиц банка к сговору;
- хищение конфиденциальной информации, касающейся кредитования; сильное давление по заказу конкурирующих организаций;
- создание для сотрудников банков ситуаций, которые в последствии используются для шантажа;
- внедрение членов организованных преступных групп в банковские структуры;
- организация банкротства или ликвидации коммерческого банка путем дискредитации, инициирования финансовой паники и востребования депозитов вкладчиками.

7.2 Криминогенные факторы в банковской сфере

В структуре внешних факторов преступности, в свою очередь, могут быть выделены две большие группы.

К первой группе относятся факторы макроуровня, то есть факторы, определяющие массовый характер преступности.

Вторую группу составляют факторы микроуровня, то есть такие, которые способствуют совершению конкретного общественно опасного деяния.

К числу детерминантов макроуровня можно отнести следующие факторы:

1. **Несовершенство правовых регуляторов общественных отношений**. Вследствие этого субъекты не защищены от недобросовестных сделок, в том числе уголовно-правовыми средствами.

2. **Неэффективность системы контроля за деятельностью банков**. Это находит проявление в недостатках при проведении бухгалтерских ревизий, низком качестве работы аудиторских служб, недостаточном уровне профессиональной подготовки банковских контрольно-ревизионных работников. Отсутствие эффективной системы контроля за деятельностью банков обусловлено во многом преобладанием государственных организаций среди учредителей при создании многих банков. С этим связана была и их слабая заинтересованность в контроле за деятельностью правления банка и эффективным использованием собственности.

3. **Относительно низкое качество аудиторской деятельности** было первоначально обусловлено слабостью государственного контроля. В частности, на первоначальном этапе деятельности аудиторских служб не было предусмотрено их лицензирование, не создана палата (служба) аудиторов. Определенную роль играет конкуренция между аудиторскими фирмами, что побуждает их более терпимо относится к выявленным нарушениям и давать нужные клиентам заключения.

4. **Неэффективность контроля за формированием уставного капитала коммерческих банков**. Так, особенно на первоначальном этапе развития коммерческих банков, получила массовое распространение практика увеличения и формирования уставного капитала за счет получения кредитов. Деятельность таких коммерческих банков связана с повышенным риском как для вкладчиков, так и для стабильности всей кредитной системы, так как повышает опасность банкротства.

5. **Недостатки контроля за правомерностью открытия счетов**. Коммерческие банки заинтересованы в привлечении денежных средств клиентов. Это является одним из факторов отсутствия в ряде случаев действенного контроля за законностью открытия счетов.

Материалы проведенных Центральным банком России проверок деятельности коммерческих банков свидетельствуют о наличии грубых нарушений правил открытия счетов и совершенных с ними операции юридическими лицами.

7.3 Классификация преступлений в банковской сфере и их характеристика

Классификация преступлений в кредитно-банковской сфере может быть осуществлена по различным основаниям в зависимости от целей изучения явления, целесообразно выделить злоупотребления, наиболее характерные для банковской деятельности.

В зависимости от субъекта в структуре преступности в кредитно-банковской сфере целесообразно различать:

7.3.1 Преступления, совершаемые руководителями банков и других кредитных организаций

1. **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, причинившее крупный ущерб. Получила распространение криминальная практика создания банков и других кредитных организаций с целью привлечения и последующего хищения денежных средств других лиц. Многочисленные лжебанки, финансовые компании причинили ущерб десяткам миллионов граждан. Особенно значительный ущерб был связан с деятельностью фирм, использующих принцип финансовых пирамид.

2. Преступления против интересов акционеров и пайщиков (мошенничества с балансовыми ведомостями).

3. Преступления против кредиторов (мошенничество).

4. Преступления, связанные с банкротством (преднамеренное банкротство, фиктивное банкротство, неправомерные действия при банкротстве).

5. Преступления против финансовой системы государства (отмывание денег, налоговые преступления).

6. Преступления против условий и порядка осуществления банковской деятельности (незаконная банковская деятельность, коммерческий подкуп).

7. Злоупотребление депозитным капиталом. Данный вид преступлений связан, как правило, с мошенническим присвоением денежных средств, привлеченных на банковские счета.

7.3.2 Преступления бухгалтерских служащих банков

Особое место занимают преступления, совершаемые с использованием методов бухгалтерского учета. Их субъектами являются ответственные сотрудники бухгалтерии. Бухгалтерские служащие по сравнению с другими категориями банковских служащих наиболее активно вовлечены в следующие незаконные операции:

1. Завышение и занижение суммы проводок по дебиту и кредиту.

2. Неправомочное списание со счетов, когда служащий действует как агент или лицо, имеющее доверенность.

3. Фиктивные вклады.

4. Счета на фиктивные лица.

5. Фиктивные проводки по счетам клиентов.

6. Отнесение чеков служащих на счета клиентов.

7. Изъятие и уничтожение чеков служащих до переноса чеков в бухгалтерскую книгу.

8. Неправомочные снятия с временно неиспользуемых счетов.

9. Незаконное присвоение комиссионных сборов.

10. Незаконное присвоение вкладов.

11. Манипуляция с процентами по сберегательным счетам. Бухгалтер, в круг обязанностей которого входит бухгалтерский учет, имеет ограниченные возможности для злоупотреблений. Однако некоторые способы, к которым

прибегают бухгалтеры, при определенных обстоятельствах могут нанести банку существенный ущерб.

В небольших банках, где бухгалтерам, ведающим индивидуальными бухгалтерскими книгами и бухгалтерскими книгами сбережений, разрешено иметь доступ к наличным деньгам, гроссбуху и другим банковским записям и документам, поле для их криминальной деятельности значительно расширяется по сравнению с крупными банками. Нечестный служащий не только достаточно свободно может получить наличные деньги, но имеет к тому же значительные возможности для утаивания своих растрат. Ему довольно просто скрыть недостачу в своем отделе и путем манипуляции по ее сокрытию в учетных документах, и наоборот.

7.3.3 Преступления, совершаемые служащими кредитных и вексельных отделов

В банковской сфере распространены следующие виды преступлений, совершаемые служащими кредитных и вексельных отделов:

1. Манипулирование процентами по сберегательным счетам (завышение фактических процентов, начисляемых на различные счета, и использования суммы, предоставленной в завышении, для компенсации фиктивных).
2. Фиктивные кредиты.
3. Необеспеченные займы предприятиям, в которых руководители и служащие банка имеют финансовую заинтересованность.
4. Займы под неадекватное и не обладающее ликвидностью (или имеющее ограниченную ликвидность) обеспечение.
5. Занижение сумм денежных сборов, ссудных процентов, скидок и завышение сумм выплаты процентов.
6. Занижение кредитовых и завышение дебетовых проводок по контрольному счету в общей бухгалтерской книге.
7. Продление срока платежа и увеличение размеров комиссий без ведома клиентов.
8. Несанкционированное освобождение залога.
9. Незаконное присвоение учетных векселей.
10. Незаконное присвоение платежей по векселям.
11. Использование в корыстных целях векселей, на которых должник проставляет бланковый индоссамент и оставляет для пролонгирования срока погашения кредита.
12. Использование неосведомленности заемщика, уже оплатившего часть суммы векселя, для понуждения его к полной оплате векселя.
13. Незаконное присвоение чековых сумм, оставленных должником для оплаты векселей по истечении их срока.
14. Подмена векселей, подписанных несостоятельными векселедателями, на имеющиеся векселя должностных лиц.

Для совершения злоупотреблений в кредитных и вексельных отделах банковские служащие чаще всего подделывают на векселях подписи клиентов. Существование поддельных векселей иногда обнаруживается во время их просмотра должностными лицами, знакомыми с подписями заемщиков.

Недобросовестные сотрудники присваивают банковские деньги путем занижения дохода, полученного в форме ссудных процентов и скидок по займам, или завышения суммы возврата процентов, когда займы погашаются досрочно.

Имеют место случаи выдачи фиктивных займов, оформленных на подставных или вымышленных получателей по несуществующим адресам или по адресам лиц, не имеющих никакого отношения к этим займам.

В течение дня или к моменту закрытия банка его служащие, подающие инкассо чеков и других документов, готовят бланки дебета и кредита, показывающие сумму, которую бухгалтер, ведущий общую бухгалтерскую книгу, должен иметь по дебету и кредиту ссудных счетов за день. Для сокрытия растраты служащие иногда занижают проводки по кредиту и завышают проводки по дебету.

7.3.4 Преступления, совершаемые служащими в транзитных отделах банка (занимаются оформлением платежей с банками-корреспондентами)

В банковской сфере распространены следующие виды преступлений, совершаемые служащими в транзитных отделах:

2. Завышение сумм по документам по сравнению с фактически переведенными в банки-корреспонденты.
3. Фиктивные проводки против остатков банков-корреспондентов.
4. Создание фиктивных счетов банков-корреспондентов.
5. Присвоение временно не используемых денежных документов.
6. Задержки в осуществлении проводок по счетам основной бухгалтерской книги.
7. Присвоение наличных денег, полученных от инкассо возвращенных документов.

В последние годы получили широкое распространение совершаемые работниками коммерческих банков правонарушения, связанные с умышленной задержкой перечислений в бюджеты, использованием этих средств для “прокрута” на валютной бирже либо в качестве кредитов для быстрых спекулятивных сделок с целью последующего присвоения и конвертации в валюту. Такие факты носят весьма распространенный характер.

7.3.5 Иные преступления, совершаемые служащими банка

В настоящее время широкое распространение получили коммерческий подкуп банковских служащих и незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну.

Наиболее часто целью коммерческого подкупа банковского работника является склонение их к выдаче кредитов с нарушением экономических нормативов, требований обеспечения возвратности кредита и других условий.

Незаконное вознаграждение дается также за выполнение иных действий:

- предоставление преимуществ при выдаче кредита;
- установление льготных процентных ставок либо освобождение от взимания процентов;
- согласие банка не проводить должной проработки всех сторон финансово-хозяйственной деятельности кредитуемого предприятия в целях установления источников погашения задолженности;

- предоставление кредита без определения конкретной цели либо с превышением предельно допустимых размеров для одного заемщика;
- выдачу кредита под застройку жилого дома без соответствующих документов о выделении земельного участка гражданам;
- в целях получения информации, составляющей коммерческую или банковскую тайну (о денежных вкладах, компьютерных программах, финансировании различных проектов).

Незаконные денежные вознаграждения за выдачу ссуд могут получать работники кредитного отдела, юридической, экономической службы, службы безопасности. Вознаграждение дается за ненадлежащую проверку кредитоспособности клиентов либо умышленное введение в заблуждение руководства банка относительно возможности клиента своевременно рассчитаться за полученные средства.

В других случаях работники банков обеспечивают изъятие полученных кредитных средств: за взятки не направляют кредитные средства по назначению в соответствии с кредитным договором, а зачисляют на расчетные счета хозяйствующих структур и даже на личные счета участников преступления.

В ряде случаев банковские служащие являются инициаторами незаконного получения и присвоения кредита, получая из похищенных средств свою долю.

7.3.6 Преступления должников (заемщиков, ссудополучателей)

Эта категория преступлений наиболее характерна для банковской сферы, поскольку кредитование является одной из наиболее массовых и одновременно уязвимых банковских операций. Преступлениями, посягающими на интересы банка при осуществлении ссудных операций, являются: мошенничество, незаконное получение кредита, а также преступления, связанные с банкротством (преднамеренное, фиктивное банкротство, неправомерные действия при банкротстве).

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

Рассмотрим подробнее сущность, основные способы и приемы совершения данных преступлений:

1. **Мошенническое получение кредита**. Основывается на представлении ложных сведений. Заемщик уже при оформлении кредита предполагает не возвращать его, имеет место умысел на завладение имуществом или приобретение права на него уже в момент осуществления действий, повлекших передачу этого имущества.

Введение в заблуждение потенциальными ссудозаемщиками банковских служащих осуществляется различными способами, которые могут быть объединены в две группы:

а) путем использования специально созданных для хищения кредитных ресурсов фиктивных предприятий;

б) путем фальсификации документов и применения иных приемов обмана, вследствие чего кредитные офицеры вводятся в заблуждение относительно возможностей и перспектив возврата полученных средств и качества обеспечения кредита.

2. **Использование фиктивных предприятий**. Специалисты выделяет следующие типичные приемы создания фиктивных предприятий:

а) создание предприятия по подлинным документам лицами, не намеревающимися заниматься хозяйственной деятельностью. Руководители такого, предприятия после получения кредита и его присвоения скрываются от кредиторов.

б) внесение в учредительные документы, необходимые для регистрации предприятия, искаженных сведений об учредителях (руководителях). Часто для этих целей используются утраченные либо похищенные паспорта граждан. После регистрации фирмы и получения кредита мошенник скрывается.

в) изготовление подложных уставов, регистрационных и иных документов с использованием подлинных печатей, ксерокопий действительных документов и иным образом.

г) регистрация предприятий на фиктивные адреса. Возможны различные модификации данного приема:

- при регистрации лжефирм указывается несуществующий адрес;
- указанная в качестве адреса квартира меняется, продается;
- перемена арендуемых в качестве офисов помещений без уведомления регистрационных, налоговых органов, контрагентов по сделкам.
- заключение за денежное вознаграждение устных соглашений с владельцами квартир об использовании их адреса в качестве юридического адреса фиктивного предприятия.

д) использование реквизитов ликвидированных предприятий с получением путем обмана согласия их руководителей.

е) похищение регистрационных документов действующих предприятий и открытие по ним расчетных счетов в банке.

ж) создание либо использование в целях хищения кредита легальных предприятий под давлением организованных преступных групп. Руководители подобных предприятий, получив по требованию преступников банковскую ссуду, передают ее преступникам либо непосредственно, либо под видом выполнения обязательств по сделке.

з) регистрация предприятий по ненадлежаще оформленным, недействительным документам по сговору с должностными лицами государственных органов, осуществляющих регистрацию предприятий.

и) использование для хищения кредитных ресурсов специально созданных предприятий, находящихся под контролем руководителя фирмы-ссудополучателя или связанных с ним лиц. Одна из возможных схем хищения кредита выглядит следующим образом: деньги тратятся не на цели, обозначенные в кредитном договоре (например, на развитие производства), а на приобретение различных ценностей для фирмы - получателя кредита (машин, дорогой оргтехники и т. п.). В дальнейшем руководитель фирмы, имея намерение присвоить полученные средства, учреждает ряд новых коммерческих структур на свое имя или на имя своих соучастников и передает эти ценности с баланса структуры - получателя кредита на балансы новых структур. Тем самым затрудняется установление принадлежности ценностей и их изъятие в целях возмещения ущерба.

С целью избежания ответственности на должности руководителей предприятий или главных бухгалтеров подбираются некомпетентные лица, часто судимые либо страдающие психическими заболеваниями, которые за определенное

вознаграждение подписывают документы, необходимые для реализации преступных схем.

3. **Злоупотребления при использовании банковских гарантий и поручительств**.

Можно выделить следующие способы злоупотреблений при данном способе обеспечения кредита.

а) фальсификация. Объектом фальсификации часто являются гарантийные письма. Для изготовления поддельных гарантийных писем используются следующие приемы:

- использование похищенных бланков предприятий с оттисками печатей;
- использование похищенных либо утерянных печатей;
- выполнение через сообщников оттисков настоящей печати на подложное гарантийное письмо одновременно с подделкой подписей руководителей предприятия;
- использование смонтированных ксерокопий бланков документов, оттисков печатей и подписей руководящих лиц;
- использование подложных писем, заверенных оттисками печатей со старыми названиями, реквизитами банком или их филиалов.

б) преступниками используется также прием предоставления поручительств несуществующим (фиктивным) поручителем.

в) представление в обеспечение возвратности кредита от имени солидных государственных или коммерческих структур гарантийных писем, полученных неправомерным путем. Известны случаи, когда преступники убеждают малознакомых или знакомых руководителей банков, страховых организаций, иных кредитных организаций выдать им гарантию для получения кредита, мотивируя это тем, что уже договорились насчет получения кредита, а банковская гарантия нужна лишь для формальности и что предприятие в данном случае не будет нести никакой ответственности. Получив гарантию, мошенники получают ссуду и присваивают ее, после чего скрываются.

4. **Злоупотребления при использовании залога в качестве обеспечения кредита**.

Типичными вариантами подобных действий являются:

а) представляется в качестве залога неполноценного имущества, действительная стоимость которого не соответствует заявленной;

б) предоставление в качестве залога имущества, не находящегося в собственности получателя кредита;

в) предоставление в качестве залога имущества, на которое не может быть обращено взыскание;

г) неоднократный залог одного и того же имущества.

5. **Иные приемы мошеннического обмана при осуществлении ссудных операций**:

а) способом обеспечения возвратности банковского кредита является страхование риска невозврата кредита. Развитие этого способа обеспечения возвратности кредита связано с совершением преступлений, связанных с подделкой получателями кредитов договоров страхования и предъявление их в банк в качестве документов, обеспечивающих возвратность получаемых кредитных средств;

б) при заключении кредитных договоров изготавливаются подложные документы, создающие видимость финансовой состоятельности (в частности, представляются ложные балансы), недостоверные бизнес-планы и технико-экономические обоснования предстоящих инвестиций за счет кредитных средств;

в) фабрикуются подложные документы в обоснование кредитного запроса, договоры о якобы заключенных сделках;

г) представляются подложные документы на право получения кредита на льготных условиях, по заниженной процентной ставке.

6. **Незаконное получение льготных условий кредитования**.

Получение льготных условий кредитования происходит как правило путем представления заведомо ложных сведений о хозяйственном положении либо финансовом состоянии.

Хозяйственное положение - это совокупность внутренних и внешних данных, характеризующих ведение экономического хозяйства предприятием, его производственную сторону дела.

Финансовое состояние - это наличие и характеристика денежных средств предприятия.

К заведомо ложным сведениям о финансовом состоянии относятся:

- сфальсифицированные бухгалтерские документы о регистрации в налоговой инспекции, в которых финансовое состояние представлено лучше, чем это имеет место в действительности (баланс - форма № 1, отчет - форма № 2 и др.);
- сфальсифицированные справки о дебиторской и кредиторской задолженности, о полученных кредитах и займах в других банках; выписки из расчетных и текущих счетов и др.

Льготные условия кредитования - это более выгодные условия, которые организация предлагает неопределенно большому количеству лиц. Льготные условия кредитования предоставляются банком по собственному усмотрению в пределах свободы кредитного договора.

К ним относятся лишь существенные условия:

- размер предоставляемого кредита;
- размер процентов за предоставленную ссуду;
- срок возврата кредита.

7. **Незаконное получение государственного целевого кредита**.

Государственный целевой кредит - это кредит, который выдает государство субъектам РФ, отраслям хозяйственного комплекса, организациям и гражданам для реализации определенных экономических программ (конверсионных, инвестиционных, технического содействия), на поддержку отдельных регионов, отраслей хозяйства (сельского, угольной промышленности), отдельных предприятий, новых форм хозяйствования (фермерство, малый и средний бизнес), для создания рабочих мест, обустройства беженцев, индивидуального жилищного строительства и т. п.

Незаконное получение государственного целевого кредита может быть обеспечено различными способами:

а) подделка документов, дающих право на получение льготного государственного кредита;

б) подделка документов о хозяйственном либо финансовом положении, о результатах проведения конкурса (если кредит выдается на конкурсной основе);

в) подделка документов, служащие обеспечением возвратности кредита (залог, гарантии муниципальных органов и т. п.) с целью получения государственного кредита.

8. **Использование государственного целевого кредита не по прямому назначению**.

Под использованием такого кредита не по прямому назначению понимаются действия, связанные с распоряжением полученными средствами в противоречии с условиями, сформулированными в нормативных актах о предоставлении государственного кредита, а также кредитного договора.

Они могут выражаться в следующем:

а) использование на цели коммерческого кредитования;

б) помещение на депозитные счета в других коммерческих банках;

в) использование в качестве взносов в создаваемые коммерческие структуры;

г) направление в виде материальной помощи своим филиалам, дочерним структурам;

д) раздача своим сотрудникам или другим лицам в виде беспроцентных ссуд;

е) использование для оплаты учебы своих детей, детей родственников, приближенных;

ж) приобретение различных ценностей (квартир, автомашин);

з) оплата поездки за рубеж;

и) погашение банковских кредитов, уплата налогов;

к) оплата аренды помещений и прочих хозяйственных расходов.

Основной причиной необоснованного предоставления кредитов и их расходования не по назначению является отсутствие при заключении договоров кредитования контроля и необходимости проверок со стороны коммерческих банков подлинности и достоверности документов заемщика, его платежеспособности, квалифицированных проверок, экономического обоснования кредитных проектов, а также дальнейшего использования полученных кредитов в соответствии с деятельностью, объявленной в Уставе заемщика.

7.4 Обеспечение возвратности кредитов службой экономической безопасности банка

Если проанализировать потери отечественных коммерческих банков, то наибольший ущерб из всех преступлений в банковской сфере наносят не хакеры (т.е. незаконные проникновения в банковские компьютерные системы), не подделки пластиковых карточек и не традиционные грабежи и похищения. Именно махинации при получении кредитов занимают "почетное" первое место.

Универсальным является утверждение о том, что профилактика гораздо эффективнее любого лечения. Это в полной мере относится и к требованиям экономической безопасности в кредитной политике банка. Однако здесь чаще всего возникают внутренние противоречия между службой экономической безопасности (СЭБ) и управлением кредитования, которые очень осложняют работу.

Позиция сотрудников управления кредитования очень проста: размещение привлеченных банком средств в виде кредитов - наиболее выгодное использование

свободных ресурсов (особенно в связи с падением доходности рынка государственных ценных бумаг).

Стремление выдать кредит на выгодных банку условиях (более высокие проценты и т.д.) или спасти показатели своего подразделения приводят к выдаче заведомо проблемных кредитов и к их неоднократной пролонгации (продлению срока возврата). В результате СЭБ подключают, когда прошли все сроки, средства давно израсходованы и их возврат очень маловероятен. Кроме того, свою задачу "кредитники" видят в лучшем случае в оценке бизнес-плана заемщика (который в расчетах всегда склонен идеализировать ситуацию по обороту полученных средств) и в правильном оформлении всего пакета документов по кредитному договору. Что касается сопровождения кредита, то оно заключается в беседах с клиентом, когда он бывает в банке, и в отслеживании регулярности погашения процентов.

В итоге сотрудники СЭБ (учитывая место их предыдущей службы) начинают подозревать, что большинство кредитов составляют умышленные, конструированные невозвраты, т.е. сговор клиента с представителями высшего менеджмента банка, замаскированный под добросовестную ошибку. Субъективность подобных убеждений сотрудников СЭБ усиливается тем, что благополучно, в срок погашенные кредиты вообще не попадают в их поле зрения, что существенно искажает общую оценку состояния дел.

Самым простым способом разрешения этих противоречий является правильно организованная работа кредитного комитета (коллективного органа, принимающего решения о выдаче кредитов). Представитель СЭБ (чаще всего - начальник) должен быть членом кредитного комитета, а каждый выдаваемый кредит проходить предварительную экспертизу СЭБ.

Что же представляет из себя подобная экспертиза? Прежде всего необходимо изучить:

1. Заемщика;
2. Проект (назначение средств);
3. Обеспечение кредита (гарантия, залог и т.д.).

Разумеется, изучение заемщика не ограничивается учредительными документами, хотя и они нередко дают интересные результаты. Так, уставный капитал АО "МММ" составлял 100000 рублей, а президенту печально известного "Нефтьалмазинвеста", гражданину одного из африканских государств было всего 22 года. Заключение первоклассной аудиторской фирмы также приносит определенные плоды. Кроме того, СЭБ учитывает:

1. **Технико-криминалистический анализ учредительных, регистрационных и иных документов на предмет установления признаков подделки** (соответствие документов общеустановленным формам). Наличие необходимых реквизитов. Четкость оттисков печатей, штампов. Отсутствие разночтении в экземплярах одного и того же документа, отсутствие подчисток, исправлений, дописок, травлении. Соответствие подписи должностных лиц: отсутствие извилистости, угловатости, штрихов, их сдвоенности, вдавленных бесцветных штрихов и др.

2. **Проверка в регистрационных, налоговых и иных органах фактов регистрации и постановки на учет**. Соответствие этих сведений представленным данным. Проверка в ОВД факта утраты паспорта и регистрации по нему предприятия.

3. **Активы заемщика** (размер уставного капитала, соотношение между собственными и заемными средсвами, вложения в недвижимость и т.д.);

4. **Состав учредителей**, наличие других фирм, возглавляемых учредителями данного предприятия; количество фирм, зарегистрированных по данному адресу; проверка соблюдения создания организации, в том числе с участием иностранного капитала. Выяснение случаев создания ООО или АО одним учредителем, а также состоящим из одного лица ("матрешка"). Холдинги (финансово-промышленные группы, иные объединения коммерческих организаций), дочерние и зависимые общества. Взаимоотношения между организациями; участие в уставных капиталах друг друга, совместное руководство (нахождение одного и того же лица на руководящих постах в разных организациях), совместная хозяйственная деятельность.

5. **Установление фактического адреса**. Действительность нахождения помещения по указанному адресу. Причина несовпадения юридического и фактического адреса. Адрес, где ранее находилась организация, где она собирается размещаться в дальнейшем. В чьей собственности находится помещение. Аренда помещения. На какой срок и когда заключена аренда. Своевременность арендной платы. Взаимоотношения учредителей с собственником или арендодателем. Квартира и ее принадлежность. Возможность договора с владельцем об ее использовании в качестве юридического адреса. Взаимоотношения владельца квартиры - работника организации и постороннего лица с учредителями или руководителями.

6. **Форма, в которой создано данное юридическое лицо** (наименее надежным является, разумеется, общество с ограниченной ответственностью);

7. **Проверка репутации клиента**:

а) судимость;

б) психические недостатки;

в) дееспособность;

г) компетентность;

д) отношение к выполнению своих обязательств в прошлом;

е) наличие имущественных претензий и долгов.

8. **Проверка соответствия бухгалтерских данных сведениям из налоговых инспекций**. Достоверность представленных сведений об обеспечении обязательств. Причины расхождений между данными складского и бухгалтерского учета и данными об остатках товарно-материальных ценностей. Отсутствие ареста или иных запретов на предмет залога, в том числе прав 3-х лиц. Кредитоспособность поручителя. Выданные им другие поручительства (кому и за что). Подлинность банковской гарантии.

9. Устан**овление наличия расчетных счетов, которыми может пользоваться заемщик**, в том числе расчетных счетов родственных предприятий, особых отношений с предприятиями и лицами, которые могут быть сообщниками клиента, либо где клиент может скрыть свое имущество.

10. **Проверка отношений с основными партнерами** по приобретению и сбыту сырья, продукции; были ли ранее факты банкротства.

11. **Время нахождения на рынке и на обслуживании в данном банке** (минимальный срок для обращения за кредитом в ряде банков - год, а то и более);

12. **Результаты обязательного выезда на объекты заемщика**, осмотр залога

и т.д.;

13. **Использование открытых и нетрадиционных источников информации** и т.д.

При оценке проекта СЭБ может осуществить проверку партнера (особенно зарубежного), оценить рынок с точки зрения его криминализации, возможности вероятных потерь при реализации продукции и т.д.

Проверка наличия залога или действительности гарантии, оценка ликвидности, "чистоты" от других обязательств также позволяет получить аргументы для вынесения окончательного решения экспертами СЭБ.

Экспертное заключение должно быть четко аргументировано. Разумеется, кредитный комитет может проигнорировать мнение СЭБ большинством голосов или даже избежать занесения в протокол мнения СЭБ по данному кредиту (например, “срочное”, “внеочередное” заседание кредитного комитета в отсутствие начальника СЭБ), однако четкое соблюдение требований к оформлению кредитного дела (отказ рассматривать без заключения СЭБ, юристов и т.д.) затрудняет подобные действия. Кроме того, в положении о СЭБ должно быть прямо указано, что "служба не несет ответственности за кредиты, выданные вопреки ее отрицательному мнению или вообще без экспертизы, и не привлекается к работе по их возврату". Соблюдение этих несложных правил сильно облегчит сосуществование сотрудников СЭБ и кредитного управления и сократит количество проблемных кредитов банка.

7.4.1 Требования к залогу

Для повышения безопасности выдачи кредита к залогу следует предъявлять определенные требования:

1. Рыночная стоимость залога должна быть достаточной для компенсации банку основного долга по ссуде (сумма кредита), всех процентов в соответствии с договором (за 1 год), а также возможных издержек, связанных с реализацией залога (пени, штрафы, судебные и прочие издержки при обращении взыскания на обеспечение). Каждый банк в индивидуальном порядке решает, как он будет определять рыночную стоимость. Существует несколько стандартных способов, когда стоимость залога устанавливается на основе:

а) покупной (балансовой) стоимости с понижающим коэффициентом, по оборудованию - за вычетом износа за период кредитования. Понижающие коэффициенты по некоторым видам имущества достигают 0,5;

б) рыночной стоимости по результатам экспертной оценки. Здесь также часто применяются понижающие коэффициенты. Многие банки требуют, чтобы оценку производили компании, которым банк доверяет. В некоторых банках экспертизу осуществляют сотрудники банка или дочерней фирмы-оценщика;

в) суммы, указанной в договоре страхования имущества, передаваемого в залог.

Необходимо определить размер издержек. Как правило, они составляют от 10 до 20% от суммы кредита, в зависимости от вида залога. Так что, планируя выдать кредит, банк должен рассчитывать сумму обеспечения, которая бы покрывала с избытком все указанные выше затраты. Не стоит забывать и про максимальную планируемую процентную ставку. Для минимизации рисков коммерческие банки,

как правило, требуют также обязательно застраховать передаваемое в залог имущество в компании, которой банк доверяет.

2. Оформление юридической документации таким образом, чтобы время, необходимое для реализации залога в случае невозврата кредита, не превышало 150 дней. Понятно, что имущество или права, передаваемые в качестве залога, должны быть ликвидными с точки зрения не только рыночного спроса, но и действующих законов. Разумеется, все документы должны быть оформлены юридически грамотно. Банк вправе попросить предоставить уставные и прочие документы партнеров, согласившихся отдать свое имущество в обеспечение кредита. Заемщик обязан предоставить документы, подтверждающие:

а) полномочия лиц, подписывающих договор по обеспечению;

б) его право собственности на имущество, передаваемое в залог;

в) отсутствие обременений на имущество (оно не находится под арестом, не передано в залог другому банку);

г) законность распоряжения помещениями, где находится залог (если в залог передаются товары, готовая продукция, сырье).

Коммерческий банк может счесть обеспечением поручительство платежеспособной компании, да еще если она предоставит ему право безакцептного списания долга со своих счетов в случае невыполнения заемщиком условий кредитного договора. Многие банки в качестве условия предоставления кредита требуют выдачи поручительства руководителей или учредителей компании-заемщика. Такое требование вряд ли покроет финансовые потери в случае невозврата кредита, но зато имеет достаточно действенный психологический аспект.

7.4.2 Изучение кредитной истории

Основное требование к заемщику здесь достаточно простое - он должен не допускать просрочек по погашению кредита, а уплату процентов не задерживать больше чем на 5 календарных дней. Если кредит был пролонгирован, учитываются причины пролонгации. У серьезного заемщика они, как правило, всегда очень уважительные и его кредитную историю испортить не могут. Требование о наличии добросовестной кредитной истории особенно важно для компаний, которые начали свою деятельность менее чем за 1 год до момента обращения в банк за кредитом и хотят получить его в размере более 50% от актива. Но и у всех остальных заемщиков качество кредитной истории, безусловно, учитывается. Есть банки, разрабатывающие свои внутренние системы оценки качества кредитной истории.

Все сказанное относится к кредитной истории, принимаемой во внимание при рассмотрении кредитной заявки. Теперь о том, какие критерии применяются к кредитной истории заемщика непосредственно в период действия кредитного договора (качество обслуживания долга).

Для определения группы риска банк должен учитывать количество и качество переоформлений договора. Переоформлением является любое изменение условий кредитного договора. Под изменением условий понимается:

а) уменьшение процентной ставки, если не была снижена ставка рефинансирования;

б) пролонгация кредита на срок, превышающий первоначальный (например, пролонгация на 4 месяца кредита, предоставленного на 3 месяца);

в) увеличение суммы кредита.

Кредитная история - важнейший нефинансовый фактор при оценке кредитной заявки. В планах развития банковской системы уже стоит создание кредитных бюро - специальных банков данных, содержащих сведения о благонадежности заемщиков. Такие бюро существуют во всех развитых странах. Ведь хорошая репутация ценится дороже всего.

Любой банк стремится к минимизации расходов по резервам, т.е. предпочитает, чтобы все предоставляемые ссуды относились к первой группе риска. Что разрешается сделать заемщику, чтобы выданный ему кредит банк отнес к стандартным ссудам?

Классификация производится в зависимости от качества обеспечения. Если кредит обеспечен, то заемщик может:

- задержать уплату процентов на 5 дней;
- допустить просрочку по кредиту до 5 дней;
- заключить дополнительное соглашение о переоформлении "без изменения условий".

А вот если кредит недостаточно обеспечен или не обеспечен вовсе, то заемщику лучше ничего вышеперечисленного не совершать.

7.4.3 Комплексная оценка кредитных рисков

Для снижения кредитных рисков банки проводят всестороннюю экспертизу кредитного проекта и заемщиков. Факторы, которые оцениваются при этом, подразделяются на три группы: правовые, финансовые и нефинансовые.

Что понимается под **правовыми критериями**, понятно. Если компания создана с нарушениями закона, ей даже расчетный счет в банке не откроют. Юристы проверяют также полномочия лиц, которые будут подписывать договоры с банком, документы по обеспечению. Получая крупный кредит, заемщик должен предоставить все необходимые решения полномочных органов о совершении крупной сделки (свыше 25% от активов на последнюю отчетную дату). Если кредит предназначен для финансирования определенного проекта, для расчетов по конкретным договорам или контрактам, то юридическая экспертиза этих документов обязательна.

Финансовые критерии - это оценка бизнес-плана, кредитоспособности по данным баланса, другим отчетным сведениям. Каждый банк применяет свою методику, свои рейтинги. Но основные показатели практически везде одни и те же. Наличие у компании убытков не всегда становится причиной для отказа в кредитовании: многие банки ориентируются прежде всего на реальные обороты. Банк обращает внимание на финансовые и юридические связи потенциального заемщика: изучает его основных партнеров (дебиторов, кредиторов, арендодателей, арендаторов), учредителей, дочерние компании. Такая информация позволяет оценить как финансовые, так и нефинансовые факторы.

Теперь о тех **нефинансовых факторах**, которые оценивает кредитный аналитик. Самый значимый из них, как отмечалось, кредитная история. Следующий фактор - оценка руководства компании: образование, стаж работы в отрасли, в данной компании. Разумеется, основной показатель для оценки руководства - финансовое состояние и репутация самой компании. Оценочным фактором является

также доступность информации: насколько охотно и быстро компания предоставляет сведения, запрашиваемые банком, допускает ли работников банка на свою территорию для осуществления проверок. Банки очень редко запрашивают информацию, на подготовку которой требуется много времени. При условии, конечно, что в компании имеется налаженный учет всех операций. Вообще "прозрачность" партнера - одно из самых важных требований при кредитовании, как и при заключении любой рискованной сделки.

Та информация, которую проверяет и анализирует служба безопасности банка, разумеется, также относится к разряду нефинансовой. Однако результаты своего анализа эта служба, как правило, не разглашает. При ее отрицательном заключении банк просто не предоставляет кредит, без объяснения причин.

В области нефинансовых факторов находятся требования Закона РФ №115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем". Закон прямо предусматривает только один случай для признания кредитной сделки подконтрольной - когда она осуществляется с лицом или организацией, зарегистрированными в государстве или на территории, в отношении которых есть сведения о незаконном производстве наркотических средств. Банк России расширил эту сферу. Сомнительными сделками он рекомендует считать предоставление кредита:

- под залог денежных средств, размещенных в банке;
- под залог драгоценных камней, ввезенных на территорию РФ;
- под обеспечение в виде гарантии банка-нерезидента на сумму, составляющую целое число (100 тыс., 1 млн. и т.п.);
- при отсутствии очевидной связи между местом деятельности клиента и его контрагентов и местонахождением гаранта;
- с процентной ставкой, существенно превышающей среднюю процентную ставку по кредитам на внутреннем и внешнем рынках.

Кроме того, о том, что компания отмывает доходы, может свидетельствовать тот факт, что информация, изложенная в заявлении клиента о предоставлении кредита, не соответствует информации и документам, полученным в ходе переговоров от представителей заемщика. На основании таких рекомендаций ЦБ банки должны сами определить для себя перечень сомнительных сделок.

Залог – это вещественная претензия на чужое движимое имущество, земельный участок, здание или претензия на право получить компенсацию от реализации заложенного имущества, если должник не может погасить свои обязательства.

Существует два вида залога:

1) при котором предмет залога может оставаться у залогодателя;

2) при котором предмет залога передается в распоряжение, во владение залогодержателю.

Поручительство – договор с односторонними обязательствами, где поручитель берет обязательства перед кредитором оплатить при необходимости задолженность по ссуде заемщика.

Гарантия – это особый вид договора поручительства, применяемый для обеспечения обязательства только между юридическими лицами, при котором ответственность гаранта носит субсидиарный характер.

Страхование ответственность заемщика за непогашение кредита. Заемщик заключает со страховщиком договор страхования на срок действия кредитного договора на основании экспертной оценки обеспеченности кредита, кредитоспособности заемщика и степени риска по реализации кредитуемого мероприятия. В случае непогашения кредита в установленные сроки страховщик выплачивает банку, выдавшему кредит, возмещение в размере от 50% до 90% непогашенной заемщиком суммы кредита, включая проценты за пользование кредитом.

Цессия. Эта переуступка оформляется специальными соглашениями или договором. Банк имеет право воспользоваться поступившей выручкой для погашения выданного кредита и уплаты процентов за него.

За рубежом, в качестве обеспечения ссуды используется также **обеспечительный вексель**, который банк требует от своего заемщика. Этот вексель не предназначается для дальнейшего оборота.

7.5 Методы обеспечения экономической безопасности кредитных организаций

Системой обеспечения экономической безопасности финансовых объектов является совокупность мероприятий и средств, обеспечивающих борьбу с деяниями, наносящими ущерб экономической деятельности финансовых объектов. Такие деяния можно разделить на внешние, внутренние и направленные против управления (Рисунок 7.2).

Из рисунка 7.2 видно, что для эффективной работы службы экономической безопасности необходимо проведение комплекса мероприятий, пресекающих нарушение работы объектов кредитно-финансовой сферы.

Выполнение мероприятий по обеспечению экономической безопасности способствует стабильному экономическому положению финансового объекта, чего требуют акционеры, государственные органы, клиенты и потенциальные инвесторы. Зашита имущественных интересов - элемент безопасности в бизнесе. Эти интересы нередко нарушаются в результате неисполнения обязательств по договорам. Одним из видов правовой защиты являются предусмотренные гражданским законом способы обеспечения исполнения договорных обязательств: залог, гарантия и т. п. Система мер обеспечения экономической безопасности банка основывается на контроле экономической деятельности финансового объекта. Использование обычного аудита не в полной мере отвечает современным требованиям, поскольку не отличается оперативностью и при возрастании объема информации сталкивается с трудностями по ее обработке.

Понятно, что нанесение ущерба деятельности финансовых объектов проводится специалистами, и поэтому борьба с ними носит прежде всего интеллектуальный характер.

Помощь в такой борьбе должны оказать средства, разработанные с использованием методов искусственного интеллекта.

Такие средства обладают тремя чрезвычайно важными качествами:

- компетентностью;
- беспристрастностью, что особенно актуально, когда речь идет о денежных средствах;

Рисунок 7.2 - Система обеспечения экономической безопасности финансовых объектов

- оперативностью работы с большим объемом информации.

Интеллектуальные средства обеспечения экономической безопасности финансовых объектов должны осуществлять контроль ежедневной и периодической бухгалтерской отчетности банка с целью определения соответствия финансовой отчетности банка его действительному положению, интерпретировать результаты контроля и давать заключения о достоверности, полноте и реальности таковой отчетности, ее соответствия действующему законодательству и требованиям, предъявляемым к ведению бухгалтерского учета, а также вырабатывать рекомендации по оптимизации деятельности финансового объекта. В случае выявления нарушений сообщать, где, когда и кем сделаны противоправные операции. Интеллектуальные средства должны выполнять следующие функции (решать следующие задачи):

- контроль финансовых операций (банковские операции, платежный оборот, денежное обращение, кредит, финансирование банковской деятельности и т. д.);
- анализ экономических нормативов деятельности финансового объекта, прогнозирование и выдача рекомендаций по управлению его деятельностью, обучение персонала;

- анализ структуры клиентов, предотвращение открытия счетов несуществующих фирм и выполнения несанкционированных финансовых операций, борьба с легализацией «теневого» капитала;
- получение и обобщение информации о конкурентах и разработка стратегии борьбы с ними.

В то же время наряду с интеллектуальными средствами должны разрабатываться и использоваться технические средства защиты.

Средства борьбы должны быть адекватны средствам совершения преступлений. Противопоставить силовым преступным действиям можно такие соответствующие силовые средства противодействия, как:

а) использование надежных средств хранения и перевозки ценностей - сейфов и инкассаторских машин;

б) совершенствование охранных систем - применение традиционных и нетрадиционных средств наблюдения, фиксирования и противодействия;

в) обучение и рациональное использование людей, осуществляющих охрану, оснащение их современными видами оружия, связи;

г) совершенствование системы охраны и взаимодействия;

д) разработка мероприятий и средств по противодействию утечке информации. Помимо таких традиционных приемов, для совершенствования охранных мероприятий следует создавать базу данных, содержащую информацию о динамике преступности, наличии, составе и направлении деятельности как преступных группировок, так и отдельных лиц, подозреваемых в преступной деятельности. Это могут быть осужденные, лица, отбывшие сроки заключения. Преступные группировки могут маскироваться под легальные предприятия или иметь в собственности несколько предприятий, на которые пало подозрение в противоправной деятельности или в получении дохода преступным путем. Источниками таких сведений должны стать статистическая информация о деятельности предприятий, информация, получаемая оперативным путем, сообщения из средств массовой информации, информация от граждан, критический анализ и обработка слухов и различных домыслов. Анализ такой информации позволит на ранних стадиях подготовки преступлений зафиксировать признаки подготовки и заблаговременно осуществить мероприятия, противодействующие планируемому преступлению.

Преступления, основанные на обмане, имеют характерную черту - отсутствие достоверной информации о создавшейся ситуации, деятельности и замыслах преступных элементов. Этим пользуются преступники, действия которых направляются на создание у служащих финансовых учреждений уверенности в правильности осуществляемых ими действий.

Средства борьбы против такой группы преступлений должны основываться на создании банка данных, моделировании деятельности финансового объекта в данной ситуации и формировании рекомендаций для принятия решения служащими финансового учреждения. Качество таких рекомендаций зависит от полноты информации и способов формирования управляющих решений. Понятно, что создать идеальную систему советов в реальных условиях невозможно, но ее разработка является актуальной и необходимой задачей.

Система мер по обеспечению безопасности деятельности финансовых объектов должна учитывать интересы всех субъектов кредитно-финансовой сферы и их клиентов. В связи с тем, что их интересы могут не совпадать, система мер не может быть универсальной.

Успешное выявление, пресечение и предупреждение экономических преступлений в кредитно-финансовой сфере возможны при осуществлении комплекса мероприятий:

1) постоянного анализа сложившейся оперативной обстановки на обслуживаемых объектах, определения перспектив и направлений дальнейшей работы;

2) расстановки личного состава СБ с учетом изменяющейся оперативной обстановки;

3) укрепления оперативных позиций в криминальной среде;

4) усиления контроля за работой СБ и строгой персональной ответственности руководителей, работающих по данной линии.

7.6 Техническое обеспечение безопасности коммерческого банка

Техническое обеспечение безопасности коммерческого банка должно базироваться на:

- системе стандартизации и унификации;
- системе лицензирования деятельности;
- системах сертификации средств защиты;
- системе сертификации ТС и ПС объектов информатизации;
- системе аттестации защищенных объектов информатизацией.

Основными составляющими обеспечения безопасности ресурсов КБ являются:

- система физической защиты (безопасности) материальных объектов и финансовых ресурсов;
- система безопасности информационных ресурсов.

Система физической защиты (безопасности) материальных объектов и финансовых ресурсов должна предусматривать:

- систему инженерно-технических и организационных мер охраны;
- систему регулирования доступа;
- систему мер (режима) сохранности и контроль вероятных каналов утечки информации;
- систему мер возврата материальных ценностей (или компенсации).

Система охранных мер должна предусматривать:

- многорубежность построения охраны (территории, здания, помещения) по нарастающей к наиболее ценной оберегаемой конкретности;
- комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- надежную инженерно-техническую защиту вероятных путей несанкционированного вторжения в охраняемые пределы;
- устойчивую (дублированную) систему связи и управления всех взаимодействующих в охране структур;

- высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию нарушителя;
- самоохрану персонала.

Система регулирования доступа должна предусматривать:

- объективное определение "надежности" лиц, допускаемых к банковской деятельности;
- максимальное ограничение количества лиц, допускаемых на объекты КБ;
- установление для каждого работника (или посетителя) дифференцированного по времени, месту и виду деятельности права доступа на объект;
- четкое определение порядка выдачи разрешений и оформление документов для входа (въезда) на объект;
- определение объемов контрольно-пропускных функций на каждом проходном и проездном пункте;
- оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц;
- высокую подготовленность и защищенность персонала (нарядов) контрольно- пропускных пунктов.

Система мер (режим) сохранности ценностей и контроля должна предусматривать:

- строго контролируемый доступ лиц в режимные зоны (зоны обращения и хранения финансов);
- максимальное ограничение посещений режимных зон лицами, не участвующими в работе;
- максимальное сокращение количества лиц, обладающих досмотровым иммунитетом;
- организацию и осуществление присутственного (явочного) и дистанционного - по техническим каналам (скрытого) контроля за соблюдением режима безопасности;
- организацию тщательного контроля любых предметов и веществ, перемещаемых за пределы режимных зон;
- обеспечение защищенного хранения документов, финансовых средств и ценных бумаг;
- соблюдение персональной и коллективной материальной и финансовой ответственности в процессе открытого обращения финансовых ресурсов и материальных ценностей;
- организацию тщательного контроля на каналах возможной утечки информации;
- оперативное выявление причин тревожных ситуаций в режимных зонах, пресечение их развития или ликвидацию во взаимодействии с силами охраны.

Система мер возврата утраченных материальных и финансовых ресурсов слагается из совместных усилий объектовых служб безопасности и государственных органов охраны правопорядка и безопасности.

Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, программных и

криптографических средств и мер по защите информации в процессе традиционного документооборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

При этом основными направлениями реализации технической политики обеспечения информационной безопасности в этих сферах деятельности являются:

- защита информационных ресурсов от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа (НСД) и специальных воздействий;
- защита информации от утечки вследствие наличия физических полей за счет акустических и побочных электромагнитных излучений и наводок (ПЭМИН) на электрические цели, трубопроводы и конструкции зданий.

В рамках указанных направлений технической политики обеспечения информационной безопасности необходима:

- реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера;
- ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы конфиденциального характера, в том числе на объекты информатики, на которых обрабатывается (хранится) информация конфиденциального характера;
- разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;
- учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль за несанкционированным доступом и действиями пользователей;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
- снижение уровня и информативности ПЭМИН, создаваемых различными элементами технических средств обеспечения производственной деятельности и автоматизированных информационных систем;
- снижение уровня акустических излучений;
- электрическая развязка цепей питания, заземления и других цепей технических средств, выходящих за пределы контролируемой территории;
- активное зашумление в различных диапазонах;
- противодействие оптическим и лазерным средствам наблюдения;
- проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств;
- предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

- обоснованность доступа, когда исполнитель (пользователь) должен иметь соответствующую форму допуска для ознакомления с документацией (информацией) определенного уровня конфиденциальности и ему необходимо

ознакомление с данной информацией или необходимы действия с ней для выполнения производственных функций;

- персональную ответственность, заключающуюся в том, что исполнитель (пользователь) должен нести ответственность за сохранность доверенных ему документов (носителей информации, информационных массивов), за свои действия в информационных системах;
- надежность хранения, когда документы (носители информации, информационные массивы) хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение;
- разграничение информации по уровню конфиденциальности, заключающееся в предупреждении показания сведений более высокого уровня конфиденциальности в документах (носителях информации, информационных массивах) с более низким уровнем конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи;
- контроль за действиями исполнителей (пользователей) с документацией и сведениями, а также в автоматизированных системах и системах связи;
- очистку (обнуление, исключение информативности) оперативной памяти, буферов при освобождении пользователем до перераспределения этих ресурсов между другими пользователями;
- целостность технической и программной среды, обрабатываемой информации и средств защиты, заключающаяся в физической сохранности средств информатизации, неизменности программной среды, определяемой предусмотренной технологией обработки информации, выполнении средствами защиты предусмотренных функций, изолированности средств защиты от пользователей.

Требование обоснованности доступа реализуется в рамках разрешительной системы допуска к работам, документам и сведениям, в которой устанавливается: кто, кому, в соответствии с какими полномочиями, какие документы и сведения (носители информации, информационные массивы) для каких действий или для какого вида доступа может предоставить и при каких условиях, и которая предполагает определение для всех пользователей автоматизированных систем информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Положение о персональной ответственности реализуется с помощью:

- росписи исполнителей в журналах, карточках учета, других разрешительных документах, а также на самих документах;
- индивидуальной идентификации пользователей и инициированных ими процессов в автоматизированных системах;
- проверки подлинности (аутентификации) исполнителей (пользователей) на основе использования паролей, ключей, магнитных карт, цифровой подписи, а также биометрических характеристик личности как при доступе в автоматизированные системы, так и в выделенные помещения (зоны).

Условие надежности хранения реализуется с помощью:

- хранилищ конфиденциальных документов, оборудованных техническими средствами охраны в соответствии с установленными требованиями, доступ в которые ограничен и осуществляется в установленном порядке;
- выделения помещений, в которых разрешается работа с конфиденциальной документацией, оборудованных сейфами и металлическими шкафами, а также ограничения доступа в эти помещения;
- использования криптографического преобразования информации в автоматизированных системах.

Правило разграничения информации по уровню конфиденциальной реализуется с помощью:

- предварительно учтенных тетрадей для ведения конфиденциальных записей или носителей информации, предназначенных для информации определенного уровня секретности.

Система контроля за действиями исполнителей реализуется с помощью:

- организационных мер контроля при работе исполнителей с конфиденциальными документами и сведениями;
- регистрации (протоколирования) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;
- сигнализации о несанкционированных действиях пользователей.

Очистка памяти осуществляется организационными и программными мерами, а целостность автоматизированных систем обеспечивается комплексом программно-технических средств и организационных мероприятий.

Защита информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН).

Основным направлением защиты информации от утечки за счет ПЭМИН является уменьшение отношения информативного сигнала к помехе до предела, определяемого "Нормами эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН", при котором восстановление сообщений становится принципиально невозможным. Решение этой задачи достигается как снижением уровня излучений информационных сигналов, так и увеличением уровня помех в соответствующих частотных диапазонах.

Первый способ реализуется выбором системно-технических и конструкторских решений при создании технических средств ЭВТ в "защищенном исполнении", а также рациональным выбором места размещения технических средств относительно направлений возможного перехвата информативного сигнала.

Второй способ реализуется в основном за счет применения активных средств защиты в виде "генераторов шума" и специальной системы антенн.

Защита информации в линиях связи.

К основным видам линий связи, используемых для передачи информации, можно отнести проводные (телефонные, телеграфные), радио и радиорелейные, тропосферные и космические линии связи.

При необходимости передачи по ним конфиденциальной информации основным направлением защиты информации, передаваемой по всем видам линий связи, от перехвата, искажения и навязывания ложной информации является

использование крипто-логического преобразования информации, а на небольших расстояниях, кроме того, использование защищенных волоконно-оптических линий связи.

Для защиты информации должны использоваться средства криптографической защиты данных гарантированной стойкости для определенного уровня конфиденциальности передаваемой информации и соответствующая ключевая система, обеспечивающая надежный обмен информацией и аутентификацию (подтверждение подлинности) сообщений.

Безопасное использование технических средств информатизации.

Одним из методов технической разведки и промышленного шпионажа является внедрение в конструкцию технических средств информатизации закладных устройств перехвата, трансляции информации или вывода технических средств из строя.

В целях противодействия такому методу воздействия на объекты информатики, для технических средств информатизации, предназначенных для обработки конфиденциальной информации, в обязательном порядке проводится проверка этих средств, осуществляемая специализированными организациями с помощью специальных установок и оборудования, как правило, в стационарных условиях в соответствии с установленными требованиями.

Вопросы для повторения темы:

1. В чем состоит сущность экономической безопасности в банковской системе?
2. Назовите принципы, на которых основана организация и функционирование системы безопасности банка?
3. Перечислите основные составляющие обеспечения экономической безопасности банковской деятельности.
4. В чем состоит сущность финансовой составляющей безопасности банковской деятельности?
5. Назовите основные угрозы финансовым и информационным ресурсам банка.
6. Какую деятельность согласно закону следует рссматривать как лжепредпринимательство?
7. В какие незаконные операции наиболее активно вовлечены бухгалтерские служащие банка?
8. В чем основное различие банковской и коммерческой тайны?
9. Перечислите основные виды злоупотреблений при использовании залога в качестве обеспечения кредита.
10. Дайте определение льготны условий кредитования. что к ним относится?
11. Что является основной причиной необоснованного предоставления кредитов и их расходования не по назначению?
12. В чем состоит основное различие целей работников кредитного отдела и службы экономической безопасности банка?
13. С какой целью в банке создается кредитный комитет? Кто в него входит?
14. Какие мероприятия выполняет СЭБ банка при проверке репутации клиента?

15. Какие требования к залогу следует предъявлять банку для повышения безопасности выдачи кредита?

16. Перечислите основные способы установления залога.

17. С какой целью многие банки в качестве условия предоставления кредита требуют выдачи поручительства руководителей или учредителей компании-заемщика?

18. Что разрешается сделать заемщику, чтобы выданный ему кредит банк отнес к стандартным ссудам?

19. Что Вы понимаете под правовыми критериями комплексной оценки кредитного риска?

20. Дайте определение залогу. Какие виды залога Вы знаете?

21. Назовите основные составляющие технического обеспечения безопасности коммерческого банка.

Литература:

1. Бекряшев А.К., Теневая экономика и экономическая преступность. - М: «ИНФРА-М» 2002г. - 153с.

2. Бугаевский А.С., «Подходы к оценке надежности потребителей финансовых услуг банка» // Финансовый менеджмент - 2002 г. - №2

3. Коган Е.А. «Оценка возможной неоплатности долговых обязательствм занмщика» // Финансы и кредит - 2003 г. - №7

4. Лисичкин Д.А. «Криминальные методы воздействия на должников и кредиторов» // доклад начальника информационно-аналитического отдела Института экономической безопасности

5. Лисичкин Д.А. «Уголовно-правовое преследование недобросовестных заемщиков и защита имущественных требований кредиторов» // доклад начальника информационно-аналитического отдела

6. Савина В. «Секреты получения кредита» // Директор-Инфо - 2002 г.

7. Тосунян Г. «Организационно-правовые проблемы повышения эффективности борьбы с финансовой преступностью в банковской сфере» // Финансовый бизнес - 2004г. – 276.

8. Экономическая и банковская безопасность/Под общ. ред. Н.Г. Краюшенко - М.: Рубикон, 2003.-346с.

Глава 8 Экономическая безопасность на рынке страховых услуг

Ключевые понятия:

Страхователь
Страховщик
Выгодопреобретатель
Объекта страхования
Фиктивный страховой случай
Инсценировщик
Инсценировка
Инсценируемое событие
Материальные следы
Суброгация

8.1 Основные положения

Развитие страхового рынка - одно из важнейших условий становления эффективной отечественной экономики. Однако созданию современной страховой индустрии препятствует множество факторов, среди которых кризисное состояние экономики, несовершенство налогового законодательства и ряд других. В настоящее время одним из наиболее деструктивных факторов является криминализация страхового рынка. Развитие страхового бизнеса, увеличение его финансовых ресурсов привлекает в эту сферу и криминально ориентированных субъектов.

Преступления в сфере страхования обладают повышенной общественной опасностью, поскольку затрудняют или блокируют выполнение его основных задач, связанных с формированием за счет денежных взносов целевого страхового фонда, предназначенного для возмещения возможного ущерба, выравнивания потерь в семейных доходах в связи с последствиями происшедших страховых случаев. Криминализация страхового рынка препятствует также выполнению страхованием таких важных функций, как повышение стабильности, ограничение экономических рисков, стимулирование предпринимательской инициативы, повышение кредитоспособности.

Проблема борьбы с преступностью при страховании актуальна для всех стран. Исследования подтверждают значительный ущерб, причиняемый преступностью в этой сфере. В ряде секторов страхования потери от мошенничества могут достигать 10-15% суммы страховых возмещений. Только французскими страховыми компаниями ежегодно по обманным декларациям о пожарах, угонах автомобилей, ограблении квартир выплачивается около 12 млрд. фр., а в Канаде эти потери составляют от 1,3 до 2 млрд. долл.

Исследования показывают, что в 10% случаев страховое возмещение либо завышено, либо выплата произведена незаконно. В общей сложности, если это переложить на клиентов, получивших возмещение от страховой компании, 2-3% от их общего числа возмещение получили обманным путем за счет средств остальных страхователей.

Хотя статистика потерь от мошенничества по России отсутствует, по мнению экспертов, российские страховщики несут не меньшие убытки. В России деятельность страховых мошенников активизируется пропорционально развитию страхования. Число экономических преступлений на страховом рынке неуклонно растет. За период с 1998 по 2003 год относительный прирост страховых преступлений составил 442,5 %, а средний ежегодный прирост -145 %.

Доля экономических преступлений на страховом рынке в массиве экономических преступлений во всей финансово-кредитной системе увеличилась в 1,7 раза с 3% в 1998 году до 5% в 2003 году.

Таким образом, привлекательность страховой сферы для российского криминалитета возрастает. Внимание преступников переносится с таких традиционных объектов преступной деятельности как банковская сфера и фондовый рынок в сферу страховых отношений.

8.2 Классификация преступлений в сфере страхования

Преступления в сфере страхования могут быть классифицированы по различным основаниям: в зависимости от формы, объекта страхования; субъектов, в

интересах которых совершается преступление; субъектов, на чьи права осуществляется преступное посягательство.

В зависимости от субъектов, в интересах которых совершаются преступные деяния, различают преступления:

1. Представителями страхователя - юридического лица;
2. Представителями страховщика;
3. Застрахованными лицами, выгодоприобретателями или страхователями - физическими лицами;
4. По сговору различных субъектов отношений страхования (например, застрахованными лицами и представителями страховщика).

8.2.1 Мошенничества, совершаемые представителями страхователя - юридического лица

Преступления в интересах страхователей совершаются самими страхователями либо в сговоре с наемными работниками страховых компаний. Целью их мошеннической деятельности является незаконное получение страхователями страхового возмещения или обеспечения.

Этот вид мошенничества может быть, в свою очередь, подразделен на два самостоятельных, в зависимости от того, страхует ли юридическое лицо свои интересы или же оно заключает со страховщиком договор страхования в пользу третьих лиц (например, своих работников).

Когда страхователь - юридическое лицо заключает со страховщиком договор о своем страховании (например, договор о страховании своего имущества или предпринимательского риска), обман может касаться:

1. **Объекта страхования**. Например, представители юридического лица (как правило, непосредственные руководители и (или) бухгалтерские работники) умышленно и безосновательно, с целью получения страхового возмещения увеличивают страховую стоимость (сумму) страхуемого имущества. На практике это достигается путем подделки бухгалтерских или иных документов или заимствования на время проведения экспертизы по оценке стоимости или количества имущества страховщиком чужого имущества и т.п. По истечении срока договора страхования или при спровоцированном самим страхователем страховом случае юридическое лицо незаконно получает страховое возмещение;
2. **Фиктивного наступления страхового случая**. Обман в данном случае заключается в том, что страховой случай не наступил, в то время как утверждается обратное. Примером может служить ситуация, при которой застрахованное имущество перевозится в другое место и укрывается и инсценируется факт его похищения неизвестными людьми (взламываются двери офиса, возможно связывание охранников, разбрасываются и частично уничтожаются или повреждаются предметы, находящиеся в помещении, вызывается милиция и т.д.). Результатом является получение юридическим лицом - страхователем незаконного страхового возмещения. В качестве яркого примера преступления можно привести инсценирование ограбления нью-йоркской фирмы ITALGOLD. Первоначально Lloyd's, бывший страховщик фирмы, выплатил этой компании 7,5 млн. долл. США страхового возмещения. Позднее Lloyd's, опираясь на показания детективов и судебных экспертов, сумела доказать, что ограбление было инсценировано самой

фирмой. Суд пришел к выводу, что страховая выплата в 7,5 млн. долл. должна быть возвращена страховщику.

3. **Осуществления страхового случая самим страхователем с целью получения страхового возмещения**. В этой ситуации застрахованное имущество, в том числе, например, недвижимость, уничтожается руководителем страхователя или его работниками для получения страхового возмещения. Содеянное квалифицируется опять-таки по-разному. Если руководитель фирмы преследует цель получения дополнительных денег для нужд фирмы (реально это возможно, когда обман имел место уже на стадии заключения страхового договора и касался страховой суммы страхуемого объекта), не собираясь эти деньги присваивать, он совершает должностное или управленческое злоупотребление и одновременно - умышленное уничтожение или повреждение имущества. При этом ущерб в должностном (служебном) преступлении определяется стоимостью выплаченного страхового возмещения, а ущерб, причиненный уничтожением чужого имущества, - его стоимостью.

8.2.2 Мошенничества, совершаемые физическими лицами

Застрахованные лица (страхователи - физические лица) совершают обманные действия или на стадии заключения страхового договора, или на стадии его исполнения - в отношении страховых случаев, или сразу на всех стадиях действия страхового договора. Выгодоприобретатели имеют реальную возможность совершить страховое мошенничество на стадии исполнения страхового договора.

На стадии заключения страхового договора со стороны застрахованных лиц (страхователей - физических лиц) возможны следующие виды обманных действий:

1. **Обман в отношении страхуемого имущества**. При этом лицо может:

а) страховать несуществующее имущество, используя для предъявления чужое имущество, взятое на время, или подделанные документы на имущество (например, на якобы находящуюся в собственности квартиру, но на самом деле принадлежащую другим лицам и всего лишь арендуемую виновным);

б) вводить в заблуждение относительно реальной стоимости страхуемого имущества, сознательно завышая ее для получения высокого страхового возмещения (обычно используются те же уловки, что и в первом случае - подменяется временно свое имущество на более дорогое чужое имущество, применяется документальный обман и т.п.);

в) страховать одно и то же имущество в размере его полной страховой стоимости у двух и более страховщиков.

В этой разновидности обмана могут присутствовать и два предыдущих вида обманных действий: лицо может дважды и более страховать несуществующее имущество или умышленно дважды и более завышать реальную страховую стоимость страхуемого имущества. Однако для квалификации содеянного как страхового мошенничества вполне достаточно только одного вида обмана - факта двойного страхования имущества. Эта разновидность обмана, однако, предполагает совершение обманных действий и на стадии исполнения страхового договора и соответственно относится к обманным действиям сразу на всех стадиях действия страхового договора.

2. **Обман в отношении других объектов страхования**. Это может быть, например, обман в состоянии здоровья застрахованного (страхователя - физического лица), при котором страхуется лицо, неизлечимо больное, как здоровый человек или инвалид I-II группы как вполне трудоспособное лицо и т.д. Для этого виновный прибегает к различным уловкам: подделывает и (или) использует подложные официальные (прежде всего, медицинские) документы, уговаривает другое лицо пройти медосмотр и т.д. Размер страхового мошенничества определяется в этом случае размером незаконно выплаченного страхового обеспечения.

На стадии исполнения страхового договора со стороны застрахованных лиц, выгодоприобретателей, страхователей - физических лиц возможны следующие виды обманных действий:

1. **Обман в наступлении страхового случая** (фиктивное наступление страхового случая). Обман здесь заключается в том, что страховой случай не наступил, в то время как утверждается обратное. Застрахованное имущество укрывается в другом месте, и инсценируется факт его похищения неизвестными людьми (взламываются двери квартиры или дома, возможно связывание членов семьи, разбрасываются и частично уничтожаются или повреждаются предметы, находящиеся в помещении, вызывается милиция и т.д.). Результатом становится получение застрахованным лицом, выгодоприобретателем или страхователем - физическим лицом незаконного страхового возмещения.

2. **Осуществление страхового случая самим застрахованным**, выгодоприобретателем или страхователем - физическим лицом с целью получения страхового возмещения. В этой ситуации застрахованное имущество (дом, дача, квартира, автомобиль и т.п.) уничтожается лицом путем поджога, взрыва и т.п. для получения страхового возмещения.

На всех стадиях действия страхового договора со стороны застрахованных лиц (страхователей - физических лиц) возможны все вышеперечисленные виды обманных действий, если они начинают совершаться при заключении страхового договора (например, обман в стоимости страхуемого имущества или в состоянии здоровья страхуемого лица) и заканчиваются обманом, связанным со страховым случаем (например, при его фальсификации).

8.2.3 Преступления в интересах страховщиков

Совершаются данные преступления руководителями страховых компаний и наемными работниками. Целью совершения данной категории мошеннических действий является незаконное присвоение страховщиками страховых взносов при отсутствии намерения выполнить свои обязательства по выплате страхового возмещения или обеспечения. Конкретные способы совершения данной категории деяний различны и могут быть объединены в несколько групп:

1. Осуществление страховой деятельности организациями, созданных с нарушением порядка создания, регистрации, лицензирования и других установленных законодательством норм.

2. Эмиссия недействительных страховых полисов и нанесение страхователям ущерба в виде лишения возможности получения страховой выплаты.

3. Разработка недобросовестным страховщиком правил и условий страхования, которые дают возможность не производить страховых выплат и

переложить ответственность на страхователя. Таким образом, страховщик, заключая страховой договор, сознательно вводит страхователя в заблуждение и обменом завладевает страховой премией.

Разновидностью данного мошенничества является завладение страховыми взносами страхователей при страховании вкладов в кредитных организациях. Сущность данного способа состоит в том, что указание в договоре вклада на то, что вклады застрахованы, не гарантирует их возвратности в случае невыполнения кредитной организацией своих обязательств перед вкладчиками. Это обещание является обманом, поскольку в страховой практике не принято страховать риск, который является управляемым для страхователя.

В ряде случаев страховая компания находится под контролем финансовой организации, принимающей вклады, и ликвидируется одновременно с не выполнившей обязательства финансовой компанией.

Используется также такой способ введения в заблуждение клиента, как наличие в договоре оговорки о вступлении договора страхования вклада в законную силу лишь после перечисления в полном объеме страховых взносов. Неуплата страхового взноса лишает вкладчиков права на компенсацию ущерба.

На практике встречаются многочисленные иные варианты введения в заблуждение страхователей. Так, в страховом полисе могут отсутствовать обязательные реквизиты, не перечисляться страховые риски, неконкретно указываться объект страхования, отсутствовать расписка держателя полиса о том, что ему известны условия страхования, которые должны прилагаться к полису, совершаться другие действия.

Таблица 8.1 – Правонарушения на страховом рынке со стороны страховщика

Способы обмана	Что делать
Страховщики предлагают клиентам огромные суммы страховых выплат. Как правило, такие компании построены по принципу „пирамид“. Рано или поздно хозяева скроются с денежками и клиенты окажутся ни с чем.	Не стоит доверять слишком заманчивой рекламе. Проценты выплат давно устоялись на столичном рынке. И если вам предлагают сумму, в несколько раз превышающую среднюю, значит, дело нечисто.
Вкладывают деньги страхователей в сомнительные финансовые операции. Результат тот же - фирма разорилась или исчезла с деньгами, оставив клиентам на память красочные полисы.	Фирма, которой можно доверять, должна несколько лет работать на рынке. Узнайте через знакомых, была ли выплачена кому-то из них страховка.
Неправомерно отказывают в страховых выплатах, пользуясь неосведомленностью клиентов. Подписывая страховой договор, рядовые граждане невнимательно вчитываются в его содержание. При пожаре, болезни, или аварии вдруг оказывается, что во всем виноват сам потерпевший. И никаких денег ему платить не собираются.	Перед тем как ставить подпись под договором, проконсультируйтесь с независимым экспертом. Образец договора вам обязаны выдать. Постарайтесь собрать как можно больше информации о фирме, с которой собираетесь заключить договор.

Преступления в интересах наемных работников совершаются ими самими. Целью совершения данного преступления является получение экономической выгоды работниками страховых организаций посредством причинения имущественного ущерба страховщикам и страхователям. Субъектами таких

преступлений являются работники среднего звена, материально ответственные лица, бухгалтеры, страховые агенты, руководителя страховых организаций.

Среди преступлений совершаемых страховыми агентами типичными являются полное или частичное присвоение страховых взносов страхователей. Руководители страховых организаций по сговору с сотрудниками бухгалтерии осуществляют хищение страховых взносов страхователей, не регистрируя страховые договоры.

Страховые операции используется в криминальной практике для уклонения от уплаты налогов, незаконного экспорта капитала, легализации доходов, полученных преступным путем.

1. Уклонение от уплаты налогов с использованием страхового оффшора. Следующая схема уклонения от уплаты налогов посредством страховых операций основана на использовании преимуществ оффшорных зон. Как правило, законодательство запрещает уменьшать налогооблагаемую базу в связи с самострахованием. В то же время страховые взносы включаются в издержки и уменьшают налогооблагаемую прибыль. Возможный вариант поведения налогоплательщика состоит в создании полностью принадлежащего ему страхового фонда. Большинство таких компаний сформировано в оффшорных зонах – юрисдикциях финансовой секретности. Используя деньги контролируемой страховой компании в налоговом убежище, налогоплательщик может перекачивать деньги из своей родной страны в оффшорное убежище, где они могут быть использованы по его усмотрению и в то же время создавать вычитаемые расходы в компании на родине.

2. Компания налогоплательщика платит страховую премию иностранной страховой компании, тем самым получая якобы налоговую скидку. Страховая компания затем перестраховывает (передает премию и страховую ответственность) второй "страховой" компанией, которая в действительности находится под контролем налогоплательщика. Его "премия" за вычетом определенного процента, удерживаемого первой страховой компанией, возвращается под его контроль и может быть инвестирована за пределами страны или возвращена в страну в форме необлагаемого налогом дохода.

3. Расторжение фиктивных страховых договоров. Данная схема используется в целях выведения безналичных средств в наличный оборот и снижения на этой основе налоговых платежей. После поступления средств предприятия на счет страховой фирмы договор по инициативе предприятия расторгается и страховые суммы возвращаются наличными. При этом возврат денег осуществляется из кассы организации – страховщика либо руководству предприятия, либо непосредственно работникам по списку.

8.3 Инсценировка как основной метод правонарушений на страховом рынке

Для осуществления планов по совершению большинства из рассматриваемых преступлений необходимо наличие трех условий:

1. Заключение договора страхования и уплата страхового взноса;
2. Инсценировка страхового события в отношении застрахованного имущества;
3. Подача заявления о страховом событии.

Сущность понятия инсценировки составляют следующие понятия:

Инсценировщик - лицо, которое создает материальную обстановку какого-либо события. Руководствуясь своей мысленной моделью этого события, инсценировщик создает идеальные следы для осуществления рефлексивного управления действиями таких лиц, от которых зависит принятие выгодного для него решения.

Инсценировка - комплекс действий по созданию материальных и идеальных следов какого-либо события, предпринимаемых инсценировщиком. Инсценировка заключается в осуществлении рефлективного управления действиями лиц, от которых зависит принятие выгодного для инсценировщика решения.

Инсценируемое событие - модель события криминального или некриминального характера, созданная инсценировщиком, восприятие которой правоохранительными органами и службой безопасности может повлиять на принятие выгодных для инсценировщика решений.

Материальные следы - вещи, предметы, оружие, документы и пр. - должны в совокупности с другими действиями инсценировщика создать убедительную картину инсценируемого события.

Создание идеальных следов в сознании других лиц преследует цель, в совокупности с материальными следами, убедить лиц, воспринимающих инсценируемое событие в его истинности. Способы создания идеальных следов: вербальные и невербальные сигналы, информационные носители, неполная и искаженная информация относительно события.

К действиям по подготовке инсценировке страхового события могут быть отнесены следующие:

- выбор страховой компании;
- подыскание объектов страхования;
- выбор места и времени инсценировки;
- заключение договора страхования;
- уплата страховых взносов и др.

Действиями по осуществлению инсценировки будут являться:

- перемещение застрахованного имущества;
- создание материальных следов страхового случая;
- создание идеальных следов события;
- ложное заявление;
- заведомо ложные показания.

Подготовка при совершении преступлений, по результатам исследований, включает в себя следующие действия.

1. **Анализ рынка страховых услуг**. Мошенники на этом этапе преследуют две цели: найти страховую компанию с наиболее выгодными для себя условиями страхования и обезопасить себя на тот случай, если служба безопасности той или иной компании тщательно проведет расследование страховых случаев. Такие действия характерны при совершении мошенничества в крупных городах, областных центрах, где рынок страховых услуг является достаточно насыщенным.

Указанные цели мошенники достигают, обращая внимание на следующие условия деятельности страховой организации:

а) престижность страховой организации;
б) срок деятельности страховой организации;
в) наличие и уровень работы службы безопасности;
г) виды страхования;

д) уровень тарифных ставок;

е) срок, в течение которого осуществляется страховая выплата;

ж) объем страховой выплаты и др.

Немаловажно для мошенников, имеется ли у них выход на определенную страховую компанию через своих знакомых, друзей, родственников.

2. **Выбор страховой организации.** Изучив условия страхования в различных страховых организациях, мошенники могут остановить свой выбор как на одной, так и на нескольких страховых фирмах. Это объясняется тем, что единого учета застрахованного имущества в российских страховых компаниях нет.

3. **Выбор страхового агента.** Данное действие производится мошенниками в некоторых случаях и обусловлено прежде всего наличием у них знакомых страховых агентов, что значительно облегчает задачу совершения преступления. Если страховой агент является знакомым мошенника, то мошеннику оказывается повышенное доверие. Часто агенты идут на определенные уступки и даже нарушают установленные правила страхования. Достаточно распространены случаи преступного сговора мошенников со страховыми агентами, которые идут на совершение преступления по корыстным и иным мотивам.

4. **Заключение договора страхования.** Наличие действующего договора страхования - необходимый элемент преступлений с целью получения страховой выплаты. Этот подготовительный этап является самым важным для мошенников, поскольку будущая инсценировка напрямую зависит от условий заключенного договора.

Данные действия мошенников имеют большое значение для органов, осуществляющих выявление и расследование указанной категории дел, потому что на этом этапе в действиях лица прослеживается наличие прямого умысла на совершение мошенничества. Это связано с тем, что мошенники заключают договор страхования, уже зная о предстоящем преступлении. Поэтому преступники используют возможность повлиять на условия договора страхования и заключить его с выгодой для себя.

Первое, что делают мошенники, это определяют вид страхования. Эти действия обуславливаются наличием у них определенного имущества. Далее определяется страховой риск, т.е. тот случай, от которого мошенник желает застраховаться. Мошенники, как правило, предусматривают в договоре страхования именно тот случай, который собираются впоследствии инсценировать. Кроме этого мошенник уделяет большое внимание следующим условиям:

- время заключения договора страхования;
- срок, с которого договор начинает действовать;
- срок окончания действия договора;
- вид, количество и оценочная стоимость застрахованного имущества;
- сумма страховой выплаты.

Следующим этапом, важным для мошенника, является *осмотр имущества* страховым агентом. Это самый ответственный момент, от которого зависит достижение цели преступления. Стоимость страховой выплаты зависит от стоимости застрахованного имущества. Наличие и стоимость объекта страхования определяются в ходе его осмотра. Поэтому мошенники стараются обмануть страхового агента при осмотре имущества, подлежащего страхованию. Обман мошенники осуществляют с помощью трех основных способов.

Первый заключается в том, что мошенник вводят в заблуждение страхового агента относительно реального собственника имущества. На самом деле имущество принадлежит иному лицу, но в договоре в качестве собственника указывается страхователь-мошенник.

Иногда лица, у которых было арендовано имущество, не знают об истинных целях мошенников, хотя чаще они вступают в сговор с ними.

Второй способ обмана заключается в том, что преступники вводят в заблуждение страхового агента относительно определенных свойств имущества. Этими свойствами могут быть: количество предметов, подлежащих страхованию; состояние и реальная стоимость имущества. Наиболее характерен данный способ обмана при страховании транспортных средств.

Особенностью третьего способа обмана страхового агента является полное отсутствие имущества в распоряжении страхователя, хотя мошенники представляют документы, часто фиктивные, подтверждающие наличие у них данного имущества. Страховой агент в таком случае фактически страхует пустоту. Известны случаи, когда мошенники ссылаются на то, что имущество (например, ценный груз) уже упаковано и находится в контейнере, и, чтобы не усложнять осмотр вынуждали страхового агента соглашаться на процедуру страхования без проведения осмотра.

Следующим этапом при заключении договора страхования является *уплата* страховой премии. Характерным на данном этапе будет то обстоятельство, что мошенники вносят страховые взносы сразу и в полном объеме. Это объясняется нежеланием мошенников откладывать осуществление преступление на сколько-нибудь продолжительный срок. Источниками выплаты страховой премии мошенниками являются:

- личные доходы мошенников;
- деньги, взятые в долг у родственников мошенников;
- деньги, взятые в долг у друзей, знакомых, сослуживцев мошенников;
- деньги, принадлежащие фирме, в которой работают мошенники;
- деньги, полученные в форме кредита, банковской ссуды.

После заключения договора страхования и выполнения его условий мошенники переходят к подготовке и осуществлению инсценировки страхового случая. Этот этап зависит от трех основных моментов:

1) вида страхования;
2) объекта страхования;
3) инсценируемого страхового случая.

Эти три основания тесно взаимосвязаны и предопределяют выбираемый преступниками способ совершения мошенничества.

8.4 Предупреждение страхового мошенничества

8.4.1 Предупреждение мошенничества на стадии заключения договора

Как говорилось выше, страхователи порой предпринимают различные действия, чтобы получить страховые выплаты обманным путем. Однако мошеннические действия могут быть если не полностью исключены, то во всяком случае число их может быть значительно снижено. Для этого в первую очередь каждый страховщик сам должен принимать меры для предотвращения мошенничества. С этой целью в страховой организации должна быть хорошо

налажена работа страховой экспертизы, организована работа по урегулированию убытков, качественная контрольно-ревизионная работа, работа по защите информации и безопасности страховой деятельности на всех этапах исполнения и заключения договора страхования.

На стадии заключения договора страхования анализируются различные статистические данные, а также другие материалы по тем или иным видам риска. Так, при страховании автотранспортных средств от угона следует проанализировать статистику угона, марки автомашин, наиболее часто подверженных угону, и т. п. с учетом чего и строить тарифную политику.

Помимо этого перед заключением договора страхования для выяснения возможных рисков и предотвращения мошеннических действий страхователи используют различные меры: обследование объектов страхования с помощью специалистов, заполнение страхователями анкет, опросных листов либо интервью с ними представителя страховщика и т. п.

Как правило, обследование осуществляется при страховании имущества. Поэтому, прежде чем его застраховать, необходимо убедиться, что оно есть в наличии и действительно принадлежит клиенту. Для этого следует запросить у него документы, подтверждающие покупку имущества, и выяснить, когда и у кого оно приобретено, числится ли на балансе у страхуемого предприятия. Более того, в ряде случаев следует попросить клиента представить справку из налогового органа о том, что данное имущество числится на балансе.

Достоинством получения страховщиком заполненных анкет, опросных листов является то, что с их помощью получают письменные подтверждения те или иные факты. В случае совершения мошенничества эти документы в качестве доказательств могут быть предъявлены страховщиком компетентным органам либо в суде.

Практикуется также выяснение обстоятельств и частоты наступления страховых случаев у потенциальных страхователей, частоты смены страхователем страховщиков. Частые наступления страховых случаев, смена страховщиков, «подозрительные» обстоятельства страхового случая и иные факты могут указывать на ненадежность потенциального клиента. При установлении таких «индикаторов» мошенничества следует провести более тщательную проверку потенциального клиента путем наведения справок, опросов и т. п.

В ряде случаев, для того чтобы «хитрый клиент» не похитил имущество у самого себя, получив при этом еще и страховку, страховщику целесообразно записать в договор страхования условия обязательной постановки сигнализации или охраны страхуемого имущества. Невыполнение этих условий должно вести к аннулированию договора. Если клиент ставил цель обмануть страховую компанию, то такие условия его, скорее всего, отпугнут, что в общем-то и необходимо для страховщика. Честным страховщикам эти условия в целом выгодны, и они идут на это.

Для того чтобы максимально точно определить характер и реальную степень наступления риска, возможный объем убытков, в страховых организациях существуют специальные эксперты - «риск-менеджеры».

Страховая экспертиза - надежная защита интересов страховых компаний, которые могут понести убытки из-за преднамеренных поджогов, хищений и других

видов мошеннических действий, а также в результате аварий и других событий техногенного характера.

Чтобы верно определить характер и реальную степень наступления риска, возможный размер ущерба, эксперты должны проанализировать максимально возможное количество различных факторов.

Страховое законодательство, предусмотрев возможность отказа страховщика в возмещении убытка при наличии определенных обстоятельств, не определило пути, формы и методы сбора информации, подтверждающей обоснованность отказа.

Решить эту задачу можно методами, присущими детективным службам. Закон РФ «О частной детективной и охранной деятельности» такую возможность предоставляет. С другой стороны, в страховой компании есть эксперт или подразделение, называемое экспертным, которые фактически выполняют следующие задачи и функции (Таблица 8.2):

Таблица 8.2 - Задачи и функции экспертного подразделения

Задачи:	1) сбор сведений, имеющих значение для правильной оценки риска в отношении объекта страхования; 2) разработка рекомендаций по снижению риска; 3) проведение контроля за состоянием объекта страхования; 4) оперативное определение обстоятельств страхового случая; 5) подготовка материалов для розыска утраченного застрахованного имущества; 6) определение размера убытка; 7) подготовка материалов по обязательствам возмещения вреда (агрессивные требования).
Функции:	1) анализируют сведения о причинах страхового случая; 2) проводят осмотр, обследование, наводят справки; 3) истребуют необходимые материалы и сведения; 4) привлекают сторонних специалистов; 5) дают рекомендации по изменению объема ответственности; 6) рекомендуют методики расследования страхового случая.

Страховая экспертиза защищает также интересы страхователей. По результатам страховой экспертизы страховая компания может предложить страхователям различные меры для предотвращения наступления страхового случая.

8.4.2 Предупреждение мошенничества на стадии страховой выплаты

Чтобы не стать жертвой мошеннических действий, работники страховых компаний устанавливают и анализируют различные материалы и сведения на стадии, предваряющей заключение договора страхования, а также в период его действия. Особенно ответственная работа ложится на плечи работника страховой компании при наступлении страхового случая. При этом значительная роль отводится специализированному подразделению по урегулированию убытков (департамент по урегулированию убытков, отдел выплат и т. п.).

Как показывает мировой опыт проведения страхования, одним из важнейших его элементов является комплексная и многогранная работа страховых компаний по урегулированию убытков. Страховые компании, обеспечивающие высокое качество этой работы, как правило, лидируют на страховом рынке. Например, на страховом рынке Франции за последние 10 лет существенно изменилась идеология большинства страховщиков. Если раньше речь шла о предоставлении клиентам

наибольшего объема услуг с большими бонусами, то в настоящее время практически все страховые продукты на рынке уравнялись и стали примерно одинаковыми. Основная тяжесть конкурентной борьбы сместилась в сферу урегулирования убытков. Дело в том, что своевременность их урегулирования напрямую сказывается на росте и постоянстве страхового портфеля страховой компании, исключает необоснованные выплаты и предотвращает страховое мошенничество.

В последнее время ряд российских страховщиков, проводящих страхование крупных и опасных рисков (это объекты энергетики, трубопроводного транспорта, экологические риски и др.), испытывает затруднения при принятии этих рисков на страхование, урегулировании убытков при возникновении страховых случаев. Для решения этих проблем в отдельных страховых компаниях создаются специализированные подразделения по урегулированию убытков (отделы выплат, дирекции по урегулированию претензий и убытков, сюрвейерские и экспертные группы), укомплектованные высококвалифицированными специалистами с опытом экспертной работы. В особо сложных случаях заключаются договоры сотрудничества с организациями, занимающимися оценочной и экспертной деятельностью. В то же время значительное количество страховых компаний не имеют специализированных подразделений по урегулированию убытков. Эта работа возложена на подразделения, обеспечивающие организацию проведения того или иного вида страхования, и на подразделения, непосредственно заключающие договоры страхования.

Эти и другие проблемы могут быть решены путем создания в страховой компании специализированного подразделения по выплатам страхового возмещения и страхового обеспечения для разработки и внедрения основных принципов и норм, на которых должны базироваться научно обоснованные методы урегулирования убытков.

Основными задачами такого подразделения являются:

1. Разработка методов урегулирования убытков;
2. Контроль правильности расчета ущерба, размера его возмещения, обоснованности выплат и сроков;
3. Учет уровня убыточности;
4. Управление рисками;
5. Обучение специалистов, занимающихся возмещением убытков;
6. Работа по внедрению программного обеспечения расчета суммы ущерба и размера его возмещения;
7. Участие в подборе специалистов.

Внутренняя структура подразделения по урегулированию убытков определяется исходя из поставленных перед ним задач, размеров обслуживаемой им территории, приоритетных для страховой компании видов страхования, количества обслуживаемых договоров страхования и других особенностей. Например, если в страховой компании создается дирекция по урегулированию убытков, она может состоять из структурных подразделений или отдельных специалистов по направлениям деятельности.

Подразделение по урегулированию убытков совместно с другими подразделениями должно обеспечить выполнение обязательств компании по всем

заключенным договорам страхования и перестрахования в области урегулирования убытков. Для этого оно:

1) организует и осуществляет контроль над работой филиалов в области урегулирования убытков;

2) рассматривает претензии по убыткам, заявленные страхователями;

3) проводит осмотр поврежденных объектов страхования и составляет необходимые документы на выплату страхового возмещения (обеспечения);

4) рассматривает претензии по расходам, произведенным с целью предотвращения убытка, сокращения его размера, а также с целью определения причин и размера убытка, претензии по общеаварийным расходам и расходам по списанию;

5) рассматривает повторные заявления страхователей, вызванные несогласием с решением страховщика об отказе в выплате страхового возмещения (обеспечения) или с его размером, сроками выплаты;

6) обеспечивает полноту данных, содержащихся в документах на выплату, качество оформления документов, их юридическую силу, обоснованность произведенных расчетов и сроков прохождения документов на выплату в соответствии с условиями конкретных правил страхования;

7) принимает решения о выплате согласно установленным лимитам;

8) обеспечивает тесное сотрудничество с другими подразделениями компании, занимающимися урегулированием убытков (отделами личного и имущественного страхования, юридическим отделом, службой защиты информации, бухгалтерией и др.);

9) ведет статистический учет результатов деятельности в области урегулирования убытков по отдельным видам страхования, по филиалам, по рискам и другим показателям;

10) анализирует уровень убыточности отдельных видов страхования по рискам, территориям и т. д. на базе данных статистического учета;

11) участвует в разработке и проведении мероприятий по минимизации убытков;

12) совместно с другими подразделениями компании проводит работу по оценке риска;

13) участвует в проведении превентивных мероприятий, направленных на предотвращение возникновения убытков, осуществляет постоянные связи с соответствующими ведомствами (ОВД, ГИБДД и др.);

14) постоянно изучает отечественную и зарубежную практику ликвидации убытков и урегулирования претензий, использования теоретических знаний в практической работе;

15) участвует в работе по внедрению новых и совершенствованию существующих видов страхования и др.

Подразделение по урегулированию убытков должно в первую очередь разработать положение о порядке рассмотрения убытков по договорам страхования в компании, предусматривающее схему прохождения документов и полномочия подразделения; комплексную программу исследования деятельности компании повлекшей убыточность заключенных договоров страхования. Оно также вырабатывает рекомендации по минимизации убытков. Необходимо также

разработать систему и методики оценки рисков при принятии их на страхование, определения размера ущерба и суммы его возмещения, предложения по формированию сети аварийных комиссаров, проведению превентивных мероприятий и др.

Концепция по урегулированию убытков должна вписываться в общую стратегию страховой компании. Эта работа должна удовлетворять требованиям законодательства и давать положительный эффект для компании.

Не ущемляя прав клиентов, компания должна снижать свои расходы на выплаты, делая тем самым свои тарифы конкурентоспособными на страховом рынке.

Опыт работы ведущих зарубежных и отечественных страховых компаний показывает, что создание в страховой компании специализированного подразделения по урегулированию убытков положительно сказывается на качестве обслуживания страхователей и на результатах деятельности самой страховой компании. Этот вопрос становится еще более актуальным в преддверии открытия российского страхового рынка для иностранных страховщиков, которым отечественные страховые компании должны и могут составить серьезную конкуренцию.

8.5 Практические рекомендации по предотвращению мошенничества

При наступлении страхового случая страхователь по договору имущественного страхования, после того как ему стало известно о страховом случае, обязан незамедлительно уведомить о нем страховщика или его представителя. Если договором предусмотрен срок и (или) способ уведомления, оно должно быть сделано в установленный срок и указанным в договоре способом.

Такая же обязанность лежит на выгодоприобретателе, которому известно о заключении договора страхования в его пользу, если он намерен воспользоваться правом на страховое возмещение. Неисполнение этой обязанности дает страховщику право отказать в выплате страхового возмещения, если не будет доказано, что страховщик своевременно узнал о наступлении страхового случая либо что отсутствие у страховщика сведений об этом не могло сказаться на его обязанности выплатить страховое возмещение.

При наступлении страхового случая страхователь подает заявление в страховую компанию. В правилах страхования может быть указано, какую информацию должно содержать заявление страхователя о страховом случае. Вместе с тем при поступлении такого заявления необходимо требовать от заявителя указания максимального объема имеющейся у него информации о событии, которое, по его мнению, содержит признаки страхового случая. В страховой компании целесообразно иметь типовую форму заявления, в котором обязательно должны быть отражены следующие данные (Таблица 8.3):

После получения заявления о страховом случае и объяснений заявителя об обстоятельствах происшедшего события страховщик анализирует эти данные в целях установления соответствия заявленных сведений субъекту и объекту страхования и страховым случаям. Действия страховщика при этом должны заключаться в следующем (Таблица 8.4).

Таблица 8.3 - Типовая форма заявления

Полные данные о заявителе и его отношение к договору страхования (страхователь; лицо, назначенное для получения страховой выплаты; представитель кого-либо из них).	
Дата и номер страхового полиса (свидетельства, сертификата, договора страхования).	
Полные данные об объекте страхования.	
Точное время, место и причина страхового случая.	
Время уведомления компетентного органа о событии, повлекшем страховой случай (если условиями договора страхования предполагается такое уведомление).	
Данные о мерах, принятых в целях предотвращения или уменьшения ущерба, причиненного страховым случаем (если обстоятельства не позволили принять такие меры, сообщается причина).	
Другие сведения (например, при нарушении заявителем срока сообщения о страховом случае, установленного договором страхования, заявитель обязан объяснить причины нарушения).	

Таблица 8.4 - Действия страховщика по установлению факта страхового случая по заявлению страхователя

Наименование документа	Требования	Контролируемые параметры
Заявление страхователя	Своевременность подачи	1. Дата регистрации в страховой компании по журналу регистрации заявлений и актов. 2. Срок по условиям страхования, в течение которого страхователь обязан заявить о страховом событии. 3. Причины, объясняющие просрочку подачи заявления страхователем.
	Соответствие заявленных сведений субъекту и объекту страхования	1. Является ли лицо, обратившееся с заявлением, страхователем либо его полномочным представителем. 2. Был ли договор страхования в силе на момент возникновения события (неуплата страховых взносов, ненаступление оговоренной даты начала страхования, истечение срока действия договора страхования, досрочное прекращение по инициативе одной из сторон либо в связи с уже состоявшейся выплатой страхового возмещения в размере страховой суммы, невнесение, очередных страховых платежей и т. д.). 3. Входит ли пострадавшее имущество в состав объекта страхования по договору (полису). 4. Предусмотрено ли договором страхования наступившее событие в объеме ответственности. 5. Наличие документального подтверждения факта и причины 6. Сопоставление места гибели или повреждения имущества с его местонахождением, указанным страхователем

Если в процессе такого анализа не установлено оснований для отклонения данного заявления и отказа в страховой выплате, то в одних случаях страховщик на основании полученных сведений и документов производит расчет суммы ущерба и осуществляет страховую выплату в виде страхового возмещения либо страхового обеспечения. В других случаях целесообразно провести дальнейшее исследование (проверку) обстоятельств страхового случая. Для этого следует принять меры к получению как можно большего объема информации из различных источников в целях ее последующего анализа для установления возможных признаков мошенничества.

Страховщик может запросить сведения, связанные со страховым случаем, у правоохранительных органов, банков, медицинских учреждений и других предприятий, учреждений и организаций, располагающих информацией об обстоятельствах страхового случая, а также вправе самостоятельно выяснять причины и обстоятельства страхового случая.

Законом «О страховании» предусмотрено, что предприятия, учреждения и организации обязаны сообщать страховщикам по их запросам сведения, связанные со страховым случаем, включая сведения, составляющие коммерческую тайну. При этом страховщики несут ответственность за разглашение таких сведений в любой форме, за исключением случаев, предусмотренных законодательством Российской Федерации.

Однако в зависимости от вида страхуемого имущества могут быть запрошены сведения и других организаций. В частности Законом предусмотрена возможность получения информации банков, что должно использоваться страховщиками. Эти сведения могут характеризовать финансовое положение страхователя. Как отмечалось выше, нередки случаи поджога имущества предприятия, которому грозит конкурсное производство (банкротство). То есть в ряде случаев страхование имущества с последующим умышленным поджогом осуществляется с целью поправить свое финансовое состояние. Анализ же сведений о движении денежных средств по расчетному счету в ряде случаев может вызвать обоснованные подозрения о «плачевном» состоянии предприятия и умышленном поджоге.

Различные документы (справки), свидетельствующие о тех или иных обстоятельствах, может представить и сам страхователь. Такие документы также могут быть приняты к рассмотрению. В то же время необходимо убедиться, что они соответствуют необходимым требованиям как по форме, так и по содержанию подписаны уполномоченным лицом, заверены печатями и т.д. Для этого необходимо осмотреть их и убедиться в отсутствии признаков подделки.

В случае возникновения каких-либо сомнений страховщик может перепроверить эти данные и убедиться в наличии полномочий и квалификации лица, выдавшего документ, в подлинности подписей и печатей. Если документы не соответствуют всем предъявляемым к ним требованиям, страховщик может отказать в страховой выплате.

Решение об отказе в страховой выплате принимается страховщиком и сообщается страхователю в письменной форме с мотивированным обоснованием причин отказа. Отказ страховщика произвести страховую выплату может быть обжалован страхователем в суде. Кроме того, суды могут признать договор страхования недействительным с момента его заключения по основаниям, предусмотренным гражданским законодательством, а также в случаях:

а) если он заключен после страхового случая;

б) если объектом страхования является имущество, подлежащее конфискации на основании вступившего в законную силу соответствующего решения суда.

Если для принятия решения об отказе или выплате страхового возмещения полученной информации недостаточно, страховщик принимает меры к получению дополнительной информации. В то же время следует учитывать, что в соответствии с ГК РФ выплата должна быть произведена в трехдневный срок после получения страховщиком всех необходимых документов. Поэтому необходимо либо провести проверку в указанный срок, либо осуществить выплату и проводить дальнейшую проверку, с тем чтобы при установлении обстоятельств, дающих право на отказ в выплате, решить вопрос о возврате этой суммы в добровольном порядке либо через судебные органы.

Поэтому страховщик может принимать меры к самостоятельному выяснению причин и обстоятельств страхового случая. В настоящее время наши крупные страховые компании создали собственные службы безопасности. Именно они и должны заниматься поиском дополнительной информации, проверкой тех или иных фактов и обстоятельств. В частности, они вправе дополнительно устанавливать лиц, являвшихся свидетелями тот или иного события, выяснять местонахождение свидетелей, указанных страхователем, в момент совершения события и т.п.

Им следует также уделять пристальное внимание таким фактам, которые довольно часто сопутствуют различным злоупотреблениям со стороны страхователей. Это:

- указание завышенной степени разрушения, завышенной суммы украденного, сгоревшего имущества, завышенной суммы ущерба от стихийного бедствия и др.;

- подмена поврежденного, похищенного, сгоревшего имущества, возможная продажа (передача) имущества или денежных средств перед наступлением страхового случая, что может в определенной степени свидетельствовать об умышленных действиях страхователя, направленных на наступление страхового случая.

Существенную для решения вопроса о выплате страхового возмещения информацию можно получить при осмотре места страхового случая (когда это возможно). Иногда страховыми случаями являются техногенные аварии на производстве, что приводит к взрывам, пожарам, выбросам токсичных, ядовитых и радиоактивных веществ, стихийные бедствия (землетрясение, оползень, наводнение, ураган, другие явления разрушительного характера) и т. п. Как правило, в таких ситуациях на месте происшествия работает комиссия либо расследование аварии или несчастного случая на производстве осуществляют правоохранительные органы. Поэтому при проверке и расследовании подобных случаев страховщики должны работать в тесном взаимодействии с такой комиссией либо правоохранительными органами.

Целью осмотра места страхового случая является:

1. Выявление и фиксация следов вредного воздействия, повлекшего за собой причинение ущерба объекту страхования или уничтожение (гибель) последнего;

2. Установление характера и причин этого воздействия;

3. Идентификация поврежденного (уничтоженного) объекта страхования, установление его состояния до страхового случая и оценка ущерба, причиненного этим случаем;

4. Установление общей стоимости имущества, указанного в договоре страхования, с указанием индивидуальных характеристик этого имущества;

5. Получение сведений о пострадавшем (пострадавших);

6. Выяснение обстоятельств несчастного случая (аварии);

7. Установление очевидцев страхового случая и их опрос;

8. Составление эскиза места происшествия;

9. Фиксация результатов осмотра места страхового случая и др.

Таким образом, на стадии страховой выплаты работник страховой компании (эксперт) в определенной степени осуществляет сбор доказательств, на основании которых могут возникнуть уголовные правоотношения.

8.6 Роль службы безопасности страховой компании в борьбе с мошенничеством

В условиях формирования и развития страхового рынка, усиления конкурентной борьбы среди страховщиков и увеличения количества мошеннических действий со стороны конкурентов и страхователей возникает потребность в специализированных подразделениях по защите информации и безопасности в структуре страховых компаний.

Служба безопасности (СБ) страховой компании представляет собой отдельное структурное подразделение компании.

Основными задачами этого подразделения являются:

- взаимодействие с правоохранительными органами и соответствующими службами безопасности;
- обмен информацией с другими службами безопасности и правоохранительными органами;
- проведение мероприятий в целях выявления, предупреждения и пресечения различного рода злоупотреблений и преступлений;
- разработка методических материалов по вопросам финансово-экономической безопасности и защиты конфиденциальной информации;
- сбор, накопление, анализ и автоматизированный учет информации по вопросам обеспечения комплексной безопасности подразделений и филиалов страховой компании;
- подготовка обобщенных данных и заключений по проблемам информации.

Основные направления работы такого подразделения следующие:

1. Предотвращение и выявление фактов хищений средств страховой организации, совершаемых путем:

а) неправомерных действий страхователей;

б) неправомерных действий партнеров;

в) злоупотреблений персонала.

2. Защита законных интересов страховой организации от неправомерных действий:

а) государственных органов;

б) недобросовестных конкурентов.

3. Обеспечение экономико-правового сопровождения деятельности страховой организации, направленной на:

а) сохранение и расширение имеющегося страхового поля;

б) анализ и принятие страховых рисков (андеррайтинг);
в) урегулирование страховых претензий;
г) выбор партнеров;
д) подбор персонала.

Примерная структура службы безопасности, способной на принятие комплекса мер, обеспечивающих защиту субъектов страхового рынка по всем направлениям, и первоочередные мероприятия по организации безопасности страховой деятельности в компании могут выглядеть следующим образом (Рисунок 8.1).

Рисунок 8.1 - Служба безопасности страховой компании

Основным содержанием деятельности СБ является систематическая информационно-аналитическая работа, которая осуществляется силами сотрудников оперативно-аналитического отдела (ОАО), укомплектованного специалистами, обладающими навыками и знаниями по сбору, систематизации и анализу информации. Отдельные авторы выделяют в деятельности СБ добывающие и информационные функции. В связи с этим функции сотрудников специального отдела подразделяются на две категории:

- получение различного рода информации для принятия необходимых решений;
- обработка полученной информации путем обобщения, классификации, анализа, организации хранения и выдачи информации.

Таким образом, оперативно-аналитический отдел (ОАО) имеет своей непосредственной основной функцией решение оперативных и аналитических задач. Деятельность сотрудника ОАО состоит в сборе, анализе и обобщении информации, которая облегчает работу СБ.

Сотрудник ОАО должен иметь опыт работы в оперативных подразделениях ОВД, ФСБ и других правоохранительных органах, быть специалистом в области

уголовного, гражданского права и арбитражного процесса. Для сотрудника юридического отдела необходимы опыт адвокатской работы, работы в предварительном следствии и в суде, а также наличие связей среди работников ОВД, прокуратуры и суда.

Современные процессы текучести кадров в системе ОВД позволяют привлекать в СБ не только пенсионеров и ветеранов но и молодых, имеющих достаточный опыт работы. Как правило, такие сотрудники обладают здоровыми амбициями, связанными с желанием проявить себя, у них достаточно жизненного тонуса для интенсивной и напряженной работы.

Претендент на должность сотрудника ОАО должен владеть компьютером и другой вспомогательной техникой, знать правила делопроизводства, иметь устойчивые деловые связи в оперативных подразделениях ОВД, без чего деятельность по предупреждению и пресечению страхового мошенничества практически невозможна. Поскольку его работа непосредственно связана с доступом ко всей информации, которой обладает СБ страховой фирмы, это должен быть проверенный человек, не замеченный в корыстных правонарушениях.

В аналитический отдел могут входить технические специалисты по программированию, силами которых зачастую разрабатываются новые либо используются действующие программные информационно-поисковые системы, необходимые для создания и ведения специальных баз данных (по персоналу, клиентам, конкурентам, отдельным известным криминальным элементам и преступным группировкам, физическим и юридическим лицам, совершившим противоправные деяния, и др.), а также для выделения из этих баз данных нужной для принятия управленческих решений информации, обработки больших массивов открытой информации, в том числе с целью подготовки специальных аналитических обзоров, дайджестов, бюллетеней тематического плана, включая бюллетени по отдельным видам преступлений и методам борьбы с ними, а также бюллетени отраслевого характера (отражающие ситуацию на страховом рынке и т. п.).

Информационно-аналитическая работа службы безопасности составляет значительную часть ее деятельности и осуществляется по следующим стратегическим направлениям:

- постоянный сбор, обработка, анализ информации о реальных угрозах для конкретного объекта, возникших либо могущих возникнуть при определенных условиях;
- систематизация и классификация признаков готовящихся противоправных посягательств, вероятных этапов их подготовки либо совершения;
- разработка прогнозов форм и способов совершения возможных противоправных деяний;
- систематизация приемов предупреждения, выявления и пресечения противоправных деяний, опыта служб безопасности в этом плане, в частности опыта взаимодействия с органами внутренних дел по пресечению преступной деятельности мошенников и др.

Первоочередные меры СБ страховой компании по организации и обеспечению безопасности проведения страховой деятельности выглядят примерно следующим образом (Таблица 8.5).

Таблица 8.5 - Первоочередные меры СБ страховой компании

Инструменты	Меры
Базы данных: 1. Собственные. 2. Объединенные. 3. Специальные.	Обращение к массивам информации.
Программа оценки и управления страховым риском с учетом мер по предотвращению мошенничества.	Проведение экспертизы, предшествующей заключению договора страхования. Проводится сюрвейером (специалистом компании совместно с представительством СБ): - устранение риска; - оценка риска (статистика и частные обстоятельства); - контроль за риском; - финансирование риска (расходы на экспертизу). Разработка мероприятий, предусматривающих конкретные указания участникам страховых отношений, позволяющих быстро действовать в непредвиденных обстоятельствах.
Превентивные мероприятия на стадии заключения договора страхования.	1. Обследование объектов страхования. 2. Проведение интервьюирования потенциального страхователя. 3. Проверка наличия и принадлежности страхуемого имущества. 4. Экспертиза документов, подтверждающих права на страхуемое имущество. 5. Изучение «страховой истории» клиента. 6. Изучение личности клиента.

Деятельность службы безопасности должна осуществляться в тесной увязке с работой других подразделений страховой компании, особенно при подготовке проектов договоров, проверке надежности клиентов, при расследовании сомнительных страховых сделок или часто встречающихся страховых случаев, при урегулировании крупных убытков, при розыске должников при возврате финансовых средств и восстановлении финансовых потерь.

Специалисты СБ проводят плановые и специальные проверки состояния информационной и финансово-экономической безопасности в подразделениях и филиалах страховой компании.

Структуры таких служб зависят от поставленных перед ними задач и могут включать в себя специализированные группы по работе с подразделениями и филиалами компании, по сбору и защите информации, по информационно-аналитической работе, по охране инкассации, офисов и руководителей страховых компаний.

8.7 Работа службы безопасности по обеспечению возмещения ущерба

Одной из статей расходов у каждой страховой компании являются дела по **суброгациям**, т.е. по возмещению ущерба, причиненного объектам страхования. Ежедневно происходит множество страховых случаев, при которых виновными признаются не страхователи, а другие лица. Поэтому одной из важнейших задач СБ является обеспечение эффективной работы по возмещению ущерба, причиненного страховой компании и ее клиентам.

Как правило, большую часть подобных случаев составляют дорожно-транспортные происшествия. Типичной является ситуация, когда виновное лицо, совершившее ДТП, в котором участвовало и транспортное средство страхователя, по различным причинам уклоняется от возмещения ущерба. Поэтому зачастую бывает очень сложно взыскать с виновного сумму ущерба и стоимость дополнительных расходов. Нередко передача материалов о возмещении ущерба в суд общей юрисдикции не дает никаких результатов.

В связи с этим можно предложить ряд рекомендаций по эффективному обеспечению возмещения ущерба.

ПРАВИЛО ПЕРВОЕ. Нужно знать наиболее распространенные способы уклонения от возмещения ущерба. Российская действительность заставляет наших соотечественников придумывать самые изощренные способы уклонения от уплаты долгов, штрафов и других принудительных выплат. Практика работы СБ страховых компаний знает несколько типичных способов ухода от возмещения ущерба:

1. Сообщение на месте ДТП ложных сведений о реальном владельце транспортного средства и о месте жительства виновного;
2. Сообщение ложных данных о Ф.И.О., месте прописки, номере телефона виновного;
3. Дача ложных обещаний об урегулировании вопроса сразу «за наличный расчет» с целью избежания вызова работников ДПС;
4. Уклонение от явки в страховую компанию и от проведения экспертизы;
5. Убеждение работников страховой компании в своей честности по отношению к уплате долга с целью получения дополнительного времени для обеспечения невозврата долга;
6. Выезд с места жительства;
7. Оформление имущества, подлежащего аресту, на родственников, друзей;
8. Вывоз имущества, подлежащего аресту, в другое место;
9. Снятие транспортного средства с учета и реализация по доверенности;
10. Сообщение ложной информации о месте работы с целью сокрытия размера заработной платы;
11. Отказ вести переговоры с работниками страховой компании;
12. Распространение ложных сведений о выезде в другой город, страну;
13. Преступный сговор с работниками службы судебных приставов.

Указанные способы противодействия возмещению ущерба страховым организациям требуют применения эффективных контрмер.

ПРАВИЛО ВТОРОЕ. Информация - 50% успеха. Для того чтобы обеспечить успешное взыскание денежных средств, необходимо обладать максимумом информации о виновном. Для этого нужно сделать следующее:

1. Обеспечить полноту получения информации на месте страхового события:
   - проверить документы виновного на месте и переписать все его данные;
   - переписать все данные транспортного средства, узнать, кому оно принадлежит;
   - сфотографировать виновного;
   - истребовать документы у ГИБДД;
   - взять домашний и рабочий телефоны виновного лица;
   - узнать место и адрес его работы;
2. Заполнить и отправить типовой запрос в ГИБДД о наличии транспортных

средств, зарегистрированных на имя виновного лица;

3. Заполнить и отправить в учреждение юстиции типовой запрос о наличии у виновного в собственности объектов недвижимости и дачных участков;

4. Заполнить и отправить в суд типовое исковое заявление о возмещении ущерба.

ПРАВИЛО ТРЕТЬЕ. Ради успеха можно пойти на уступки. Как показывает практика, люди неохотно расстаются с деньгами, даже если понимают, что платить все равно придется. Однако при наличии шанса заплатить меньше редкий здравомыслящий человек этим шансом не воспользуется. Поэтому для получения большей части долга в возмещение ущерба можно уступить меньшую часть. Например, предложения виновному об уплате только 2/3 общей суммы долга, часто воспринимаются позитивно и люди выплачивают большую часть долга, экономя время и затраты страховой компании. Естественно, виновному необходимы гарантии, что остальную часть долга с него не потребуют. Поэтому следует заготовить типовой бланк соглашения о возмещении ущерба в неполном размере.

ПРАВИЛО ЧЕТВЕРТОЕ. Законы рыночной экономики суровы, но справедливы. Если человек признан виновным в причинении ущерба другому лицу или организации, он должен честно исполнять обязанности должника. Однако такое бывает не часто. Для побуждения лица возместить ущерб следует поставить в известность его родственников и близких о наличии у него денежного долга и о том, что в случае непогашения долга возможен судебный процесс. Во многих семьях денежные проблемы обсуждаются совместно. Поэтому подобная информация может быть обсуждена на «семейном совете», который примет правильное решение, обязав виновного вести себя достойно.

ПРАВИЛО ПЯТОЕ. Охотник, умеющий ждать, - хороший охотник. Профессиональные должники - это особая группа людей, которые применяют весь арсенал тайного агента разведки. Они представляются по телефону другим именем, не отвечают на телефонные звонки, не открывают дверь и даже иногда меняют внешность. Они четко знают, что две-три недели такой скрытной жизни обеспечат им несколько месяцев покоя. Поэтому нельзя давать таким должникам шансы вас обмануть. Для этого следует знать способы обнаружения должника:

- контрольные телефонные звонки ранним утром и поздним вечером;
- контрольные посещения квартиры в выходные и праздничные дни;
- оставление в почтовом ящике «контрольных посланий»;
- установление места нахождения должника через соседей;
- обращение к кому-нибудь из соседей должника с просьбой позвонить, когда он появится;
- посещение места работы должника с целью установить место его нахождения.

Естественно, что сотруднику СБ достаточно сложно самому тратить время на розыск подобных должников. Для такой работы подойдут студенты-практиканты, которым следует выдать удостоверение страховой компании и заключить с ними договор о вознаграждении в виде процентов от взысканных долгов.

ПРАВИЛО ШЕСТОЕ. Жадность - один из самых распространенных пороков. Недаром говорят, что психология - основа всех поступков. Интересный ход был придуман сотрудниками СБ одной из страховых компаний. Как правило, компания отправляла должникам досудебные предупреждения с целью побудить их

возместить ущерб в такой-то сумме. Расчет суммы производился с учетом реального ущерба плюс стоимость автотехнической экспертизы. Обычно 80-85% досудебных предупреждений оставались без ответа, а должники скрывались либо уклонялись от переговоров с работниками страховой компании. Однако когда в тексте досудебного предупреждения появлялась сумма, вдвое превышающая реальный ущерб, должники стали сами приходить в компанию «для выяснения отношений». Там с ними проводилась беседа с целью убеждения добровольно возместить ущерб.

Вопросы для повторения темы:

1. Назовите основные группы правонарушений страхователей - юридических лиц.
2. В какие группы объединяют преступления в интересах страховщиков?
3. Гарантирует ли страхование вкладов в кредитных организациях их возвратность в случае невыполнения кредитной организацией своих обязательств перед вкладчиками?
4. Какой метод правонарушения является основным на страховом рынке?
5. В чем заключается метод инсценировки?
6. Перечислите все способы создания идеальных следов, используемые при инсценировке страхового случая.
7. Какие условия деятельности страховой организации являются для мошенников существенными при анализе рынка страховых услуг?
8. Какой подготовительный к инсценировке этап является самым важным для мошенников и почему?
9. Назовите основное достоинство получения страховщиком заполненных анкет, опросных листов.
10. Каких экспертов привлекают страховые компании для того, чтобы максимально точно определить характер и реальную степень наступления риска, возможный объем убытков?
11. Перечислите задачи и функции экспертного подразделения страховой компании.
12. Какому специальному подразделению страховой компании отводится главная роль при наступлении страхового случая?
13. На основе каких факторов выбирается внутренняя структура подразделения по урегулированию убытков?
14. Что в обязательном порядке должно отражаться в типовой форме заявления о наступлении страхового случая?
15. В каких случаях договор страхования может быть признан недействительным?
16. В какой срок должна быть произведена выплата после получения страховщиком всех необходимых документов?
17. С какой целью производится осмотр места страхового случая?
18. Какие основные направления работы службы безопасности страховой компании?
19. Какие функции выполняет оперативно-аналитический отдел?
20. По каким стратегическим направлениям осуществляется информационно-аналитическая работа службы безопасности страховой компании?
21. Дайте определение понятию «субригация».

22. Перечислите основные способы ухода от возмещения ущерба.

Литература:

1. Алгазин А.Н., Галагуза Н.Ф., Ларичев В.Д., Страховое мошенничество и методы борьбы с ним. - М: Дело. 2003г. - 512с.

2. Бекряшев А.К., Теневая экономика и экономическая преступность. М: ИНФРА-М. 2000г. - 141с.

3. Качалова Е.Ш., «Региональное страхование в системе экономической безопасности Российской Федерации» // Финансы - 2003г. - №4.

4. ФЗ РФ от 27.11.92 № 4015-1 «Об организации страхового дела в РФ» (с изменениями и дополнениями).

Глоссарий

Аваль – вексельное поручительство третьего лица, по которому авалист принимает ответственность за выполнение обязательств кем-либо из обязанных по векселю лиц - акцептантом, индоссантом, векселедателем. Оформляется чаще всего гарантийной надписью на векселе.

Адсорбция - полное слияние или поглощение (это означает, что из двух вступивших в сделку структур на рынке остается только одна).

Акцепт – согласие на оплату и принятие на себя обязательства уплатить по векселю при наступлении срока платежа.

Акция - документ, свидетельствующий о внесении определенной части в капитал акционерного общества, который дает право на получение дохода и формальное участие в управлении предприятием.

Акцептант (трассат) – лицо, подписывающее вексель-тратту.

Акционерный капитал – стоимость выпущенных компанией акций как привилегированных, так и обыкновенных.

Аналитики покупатели – аналитики, работающие на взаимные и хеджевые фонды, которые покупают ценные бумаги для себя.

Аналитики продавцы – аналитики, работающие на инвестиционные банки и компании, которые оказывают брокерские услуги сторонним инвесторам.

Андеррайтер – лицо, организующее подписку на ценные бумаги.

Андеррайтинг – покупка ценных бумаг инвестиционными институтами новых выпусков с целью последующей продажи.

Аппаратные средства защиты - это непосредственно встроенные в компьютер системы передачи данных или оборудованные в виде самостоятельных приспособлений устройства, которые служат для внутренней защиты структурных элементов компьютерной техники.

Асимметричное шифрование – метод, при котором для шифрования используется один ключ, для расшифровки – другой.

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

Безопасность - состояние объекта (в нашем случае -предприятия) в системе его связей с точки зрения способности к устойчивости (самовыживанию) и развитию в условиях внутренних и внешних угроз, действий непредсказуемых и трудно прогнозируемых факторов.

Белый рыцарь и белый сквайр - способы защиты от недружественного поглощения, когда для поглощения приглашается дружественный акционерам инвестор. При выборе способа защиты белый рыцарь корпорация-цель пытается помешать "недружественному захвату" путем осуществления дружественного поглощения, продавая свой контрольный пакет акций дружественной менеджменту корпорации. Защита белый сквайр отличается от защиты "белый рыцарь" тем, что белый сквайр не получает контроля над целью поглощения. Дружественная к менеджменту компания - белый сквайр покупает по предложению цели поглощения крупный пакет акций на "условиях невмешательства".

Бланк – лист бумаги с оттиском углового или центрального штампа, либо с напечатанным любым способом текстом (или рисунком), используемый для составления документа.

Бланк строгой отчетности – бланк, содержащий номер (серию), зарегистрированный одним из установленных способов и имеющий специальный режим использования.

Брокер – член фондовой биржи, действующий как посредник, выполняет операции по купле-продаже ценных бумаг по заявкам клиентов.

Варрант – свидетельство, дающее его владельцу право покупки ценных бумаг новых выпусков по установленной цене в течение определенного времени или бесконечно. Иногда это свидетельство продается отдельно либо вместе с первичной ценной бумагой.

Вексель – письменное долговое обязательство строго установленной законом формы, которое выдается заемщиком (векселедателем) кредитору (векселедержателю) и предоставляет право векселедержателя требовать с заемщика уплаты к определенному сроку суммы займа и вознаграждения.

"Взлом" извне – метод проникновения, при котором преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий.

"Взлом" изнутри: – метод проникновения, при котором преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля.

Гарант – поручитель, который гарантирует выполнение обязательств по ценным бумагам.

Гарантия – это особый вид договора поручительства, применяемый для обеспечения обязательства только между юридическими лицами, при котором ответственность гаранта носит субсидиарный характер.

Государственная облигация – облигация, выпускаемая государственными органами власти для привлечения необходимых средств по выполнению государственных задач.

Государственный целевой кредит - это кредит, который выдает государство субъектам РФ, отраслям хозяйственного комплекса, организациям и гражданам для реализации определенных экономических программ (конверсионных, инвестиционных, технического содействия), на поддержку отдельных регионов, отраслей хозяйства (сельского, угольной промышленности), отдельных предприятий, новых форм хозяйствования (фермерство, малый и средний бизнес), для создания рабочих мест, обустройства беженцев, индивидуального жилищного строительства и т. п.

Депозитарная деятельность – оказание услуг по хранению сертификатов ценных бумаг и учету перехода права собственности на ценные бумаги. Для учета ценных бумаг открывается в депозитарии счет "депо".

Депозитный сертификат – письменное свидетельство о депонировании денежных средств в банке, удостоверяющее право вкладчика на получение вложенных средств и вознаграждения.

Держатель ценных бумаг – юридическое или физическое лицо, владеющее ценными бумагами.

Держатель (владелец) информации - организация или отдельное лицо (например, пользователь системы), которое обладает ценной информацией и использует ее для своих целей.

Залог – это вещественная претензия на чужое движимое имущество, земельный участок, здание или претензия на право получить компенсацию от реализации заложенного имущества, если должник не может погасить свои обязательства.

Защита Пэкмена - способ защиты от недружественного поглощения, который заключается в контрнападении корпорации-цели поглощения на корпорацию-агрессора в случае попытки жесткого поглощения (корпорация-цель делает встречное тендерное предложение акционерам корпорации-покупателя на выкуп контрольного пакета ее акций).

Защита от "недружественного поглощения" - это действия менеджмента и/или владельцев цели поглощения, направленные на предотвращение попыток ее приобретения или установления определенной степени контроля.

Именная ценная бумага – ценная бумага, зарегистрированная в реестре на имя держателя бумаги.

Индоссамент – передаточная надпись на ценной бумаге, свидетельствующая о переходе прав по этой бумаге к другому лицу.

Инсайдер – это лицо, располагающее служебной информацией.

Инсценировка - комплекс действий по созданию материальных и идеальных следов какого-либо события, предпринимаемых инсценировщиком. Инсценировка заключается в осуществлении рефлективного управления действиями лиц, от которых зависит принятие выгодного для инсценировщика решения.

Инсценировщик - лицо, которое создает материальную обстановку какого-либо события. Руководствуясь своей мысленной моделью этого события, инсценировщик создает идеальные следы для осуществления рефлексивного управления действиями таких лиц, от которых зависит принятие выгодного для него решения.

Инсценируемое событие - модель события криминального или некриминального характера, созданная инсценировщиком, восприятие которой правоохранительными органами и службой безопасности может повлиять на принятие вы годных для инсценировщика решений.

Источник информации - организация или отдельное лицо (например, заказчик), которое поставляет информацию или к которому относится информация.

Клиринг – система расчетов по взаимным требованиям по сделкам с ценными бумагами.

Клиринговая палата – биржевой или межбиржевой орган, осуществляющий расчеты между участниками биржевых сделок на основе зачета взаимных требований.

Коммерческая тайна, в соответствии с гражданским законодательством РФ, это информация которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на

законном основании и обладатель принимает меры к охране ее конфиденциальности.

Компенсационные парашюты - включаемые в контракты менеджеров условия, гарантирующие значительные выплаты этим менеджерам в случае "недружественного поглощения" или "не согласованного с менеджерами" поглощения.

Контрольный пакет акций – количество акций, владение которыми обеспечивает преимущественное право реализовывать свои идеи развития предприятия и обеспечивает контроль за деятельностью предприятия.

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

Концепция безопасности организации - выражает систему взглядов на проблему безопасности на различных этапах и уровнях предпринимательской деятельности, а также основные принципы, направления и этапы реализации мер безопасности.

Криптографические средства защиты - это средства защиты данных при помощи криптографического преобразования, то есть преобразования данных шифрованием.

Криптография - наука, изучающая принципы, средства и методы преобразования данных с целью сокрытия их содержания, предотвращая, таким образом, их несанкционированное использование или скрытую модификацию.

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, причинившее крупный ущерб.

Лицензия – разрешение, выдаваемое компетентными органами власти на ведение операций с ценными бумагами. Таким органом в настоящее время является Федеральная комиссия по ценным бумагам.

Льготные условия кредитования - это более выгодные условия, которые организация предлагает неопределенно большому количеству лиц. Льготные условия кредитования предоставляются банком по собственному усмотрению в пределах свободы кредитного договора.

Материальные следы - вещи, предметы, оружие, документы и пр. - должны в совокупности с другими действиями инсценировщика создать убедительную картину инсценируемого события.

Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.

Маскираторы - наиболее распространенный и наименее устойчивый к декодированию класс приборов.

Межсетевые экраны - это локальное или функционально-распределительное программно-аппаратное средство, реализующее контроль за информацией, поступающей в компьютер или выходящей из него.

Мошенничество - преступление, связанное с хищением чужого имущества или приобретением права на чужое имущество путем обмана или злоупотребления доверием. Мошенничество является формой хищения.

Необратимое шифрование – метод используется при шифровании паролей: зашифрованный текст записывается в память, далее сравниваются зашифрованные строки текста, при этом данные не могут быть воспроизведены.

Несанкционированный доступ к информации - преднамеренные, противоправные действия злоумышленников с целью получения охраняемых сведений.

Номинальный держатель – лицо, которое держит ценные бумаги, не являясь их владельцем, работает от своего имени, но в интересах другого лица.

Облигация – ценная бумага, являющаяся свидетельством о предоставлении займа, дает ее владельцу право на получение определенного дохода (процентного, дисконта), но не дает права голоса. По истечении срока заем подлежит возврату держателю ценной бумаги.

Обеспеченные облигации – облигации, обеспеченные имеющимися активами или ценными бумагами.

Объект безопасности предприятия - степень устойчивости и развития предприятия, его способность противостоять угрозам.

Операционные преступления - совершаются операторами ЭВМ, периферийных устройств ввода информации в ЭВМ и обслуживающими линии телекоммуникации.

Организационное обеспечение - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становятся невозможными или существенно затрудняются за счет проведения организационных мероприятий

Поглощение – приобретение контрольного пакета акций одной акционерной компании другой.

Поручительство – договор с односторонними обязательствами, где поручитель берет обязательства перед кредитором оплатить при необходимости задолженность по ссуде заемщика.

Правовое обеспечение - это совокупность норм права, определяющих общественные отношения, которые возникают в процессе деятельности людей по безопасному использованию компьютерной техники для обработки информации.

Приборные методики - это комплексные процедуры с использованием сложных технических устройств, которые предназначены для всесторонней оценки психофизиологических характеристик испытуемых лиц.

Программные средства защиты - это соответствующие процедуры, входящие в состав программного обеспечения систем обработки данных или самостоятельное программное обеспечение, входящее в состав комплексов и систем аппаратуры контроля.

Пролонгация векселя – продление срока действия векселя.

Проспект эмиссии – документ, представляемый в государственные инстанции с целью получения разрешения на выпуск ценных бумаг. Размещается вся информация о

будущем использовании привлекаемого капитала, о состоянии предприятия для потенциальных инвесторов.

Разглашение - сообщение, передача, предоставление, пересылка, опубликование, утеря и оглашение любыми иными способами конфиденциальной информации лицам и организациям, не имеющими права доступа к охраняемым секретам.

Реестр -собой список зарегистрированных владельцев с указанием количества, номинальной стоимости и категории принадлежащих им именных ценных бумаг, составленный по состоянию на любую установленную дату и позволяющий идентифицировать этих владельцев, количество и категорию принадлежащих им ценных бумаг.

Реинкорпорация - переоформление учредительных документов в другой регион (перенос юридического адреса), где существуют более жесткие антимонопольные требования, чем по текущему месту регистрации.

Рекапитализация высшего класса - метод защиты от недружественного поглощения, при котором все эмитированные компанией акции делятся на два класса: акции с обыкновенным правом голоса (низший класс акций) и акции с повышенным правом голоса (высший класс акций). Обычно акции низшего класса голосуют по принципу "одна акция - один голос", а акции высшего класса - "одна акция - десять голосов".

Реструктуризация активов - продажа и покупка активов, которая совершается для того, чтобы сделать объект поглощения менее привлекательным для "агрессора".

Рынок ценных бумаг - совокупность экономических отношений по поводу выпуска и обращения ценных бумаг.

Рыночный портфель – совокупность ценных бумаг разного вида и разных компаний. Используется при управлении пакетом ценных бумаг, доходность портфеля должна быть близка к доходности рынка в целом.

Симбиоз - взаимопроникновение двух структур: это может быть обмен крупными пакетами акций, ведущий к объединению ряда операций на финансовых рынках, взаимодополнение продуктового ряда и т.п.

Симметричное шифрование – метод, при котором для шифрования и расшифровки используется один и тот же ключ.

Система безопасности предприятия - совокупность научной теории его безопасности, политики и стратегии безопасности, средств и методов обеспечения безопасности и концепции безопасности предприятия

Служба безопасности предприятия - его структурное формирование, осуществляющее в рамках законодательства и собственного устава меры по предотвращению и пресечению угроз интересам своего учредителя.

Спекулянт – лицо, которое играет на бирже, получает доход на разнице в ценах и принимает на себя большой риск.

Спекуляция - торговля ценными бумагами с целью получения прибыли за счет разницы их курсов.

Соглашение о невмешательстве (стоп-соглашение) - контракт, который заключается между менеджментом компании-цели поглощения и крупным

акционером, согласно которому этот крупный акционер обязуется не владеть контрольным пакетом акций на протяжении определенного времени.

Суброгация – возмещение ущерба, причиненного объектам страхования.

Тендерное предложение – публичное предложение держателей акций одной компании купить акции у держателей акций другой корпорации или организации на определенных условиях и имеющее силу определенное время. Держателей акций просят предлагать свои акции по определенной цене, как правило, выше рыночной, при условии предложения максимального количества акций.

Трансфер-агент - юридическое лицо, являющееся агентом регистратора и выполняющее функции по сбору информации для внесения изменений в реестр, передаче этой информации регистратору, а также по оформлению и выдаче документов, удостоверяющих право собственности на ценные бумаги.

Трассант – векселедатель переводного векселя. Отвечает за акцепт и платеж по векселю.

Трассат – лицо, акцептующее вексель-тратту и обязующееся уплатить по переводному векселю при наступлении срока платежа.

Трассирование – выставление переводного векселя.

Тратта – письменный приказ кредитора должнику уплатить определенную сумму третьему лицу. Обязательство должника начинает действовать с того момента, как он акцептует вексель.

Тяжба - способ защиты от недружественного поглощения, при котором получение предложения о поглощении ведет к возбуждению различных судебных исков со стороны корпорации-цели. При этом корпорация-покупатель обвинялась в нарушении всевозможных видов законодательства, включая природоохранное.

Угроза безопасности предприятия - потенциально или реально возможное событие, действие, процесс или явление, которое способно нарушить его устойчивость и развитие или привести к остановке его деятельности.

Уивинг - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение.

Условие справедливой цены - способ защиты от недружественного поглощения, при котором происходит внесение в устав корпорации-цели оговорки, определяющей условия выкупа более 20% (возможно, более 30%) голосующих акций.

Условие супербольшинства - способ защиты от недружественного поглощения, при котором происходит внесение в устав корпорации - цели оговорки, предусматривающей установление высокого процента голосов, необходимого для принятия решения о слиянии.

Устав - правовой акт, определяющий свод правил, регулирующих деятельность организации, её взаимоотношения с другими организациями и гражданами, права и обязанности в определенной сфере её деятельности.

Утечка информации - неконтролируемый выход охраняемых сведений за пределы организации или круга лиц, которым они были доверены.

Учет векселей – покупка банком или другой финансово-кредитной организацией векселей до истечения срока погашения. Цена покупки ниже цены погашения на величину дисконта.

Финансовое состояние – это наличие и характеристика денежных средств предприятия.

Фоун-фрейкинг – использование компьютера для проникновения в коммутационную телефонную систему с целью незаконного пользования услугами по предоставлению междугородной телефонной связи.

Хозяйственное положение – это совокупность внутренних и внешних данных, характеризующих ведение экономического хозяйства предприятием, его производственную сторону дела.

Целевой выкуп - способ защиты от недружественного поглощения, при котором компания-цель поглощения делает прямое тендерное предложение внешнему инвестору или группе инвесторов, которые уже владеют крупным пакетом ее обыкновенных акций и могут представлять потенциальную угрозу. Выкуп производится со значительной премией по сравнению с рыночным курсом акций.

Ценная бумага – документ, удостоверяющий с соблюдением установленной формы и обязательных реквизитов имущественные права, осуществление или передача которых возможны только при его предъявлении..

Шумогенераторы – устройства, создающие постоянные помехи (шумы), которые затрудняют или делают работу подслушивающих устройств невозможной.

Эмиссия – выпуск в обращение ценных бумаг.

Эмитент – субъект (государственные органы власти, банки, предприятия, физические лица и т.д.), выпустивший ценные бумаги.

"**Ядовитые пилюли**" - способ защиты от недружественного поглощения, при котором эмитированные корпорацией-целью права, размещенные между ее акционерами и дающие им право на выкуп дополнительного количества обыкновенных акций компании при наступлении определенного события.