МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА С.П. КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (СГАУ)

Комплексное обеспечение информационной безопасности автоматизированных систем

Электронный учебно-методический комплекс
по дисциплине в LMS Moodle

САМАРА
2012

УДК 004
К 637

Автор-составитель: **Моисеев Александр Иванович**

Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle / Минобрнауки России, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т); авт.-сост. А. И. Моисеев. - Электрон. текстовые и граф. дан. - Самара, 2012. – 1 эл. опт. диск (CD-ROM).

В состав учебно-методического комплекса входят:

1. Курс лекций.
2. Методические указания по выполнению практических занятий.
3. Вопросы к экзамену.
4. Тесты по дисциплине.

УМКД «Комплексное обеспечение информационной безопасности автоматизированных систем» предназначен для студентов факультета информатики, обучающихся по направлению подготовки специалистов 090303.65 "Информационная безопасность автоматизированных систем" (специалитет) в 9 семестре.

УМКД разработан на кафедре ГИиИБ.

Глава 1. Концепция построения системы безопасности предприятия

1.1. Определение и основные понятия системы безопасности

Под системой безопасности предприятия в настоящее время понимается организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз [13]. Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только система безопасности. Опасности – это возможные или реальные явления, события и процессы, способные нанести моральный или материальный ущерб предприятию и предпринимательской деятельности.

Опасность способна приобретать различные формы. Она может быть в виде намерений, планирования действий и их реализация с целью уничтожения, ограбления, изменения, ослабления и т. д. Понятие "угроза" родственно понятию "опасность". Угроза – это опасность на стадии перехода из возможности в действительность.

Угроза – потенциально возможное или реальное действие злоумышленников, способных нанести моральный, материальный или физический ущерб персоналу. Различают внутренние и внешние угрозы,которые могут быть направлены на персонал, материальные, финансовые и информационные ресурсы (рис. 1.1).

Рис. 1.1. Виды угроз безопасности предприятия

Как и любая система, система безопасности предприятия имеет свои цели, задачи, методы и средства деятельности, которые формируются в зависимости от конкретных условий.

Целями системы безопасности являются [12]:

. защита прав предприятия, его структурных подразделений и сотрудников;

. сохранение и эффективное использование финансовых, материальных и информационных ресурсов;

Подпись: Ознакомление с охраняемыми сведениями. Модификация информации с криминальными целями. Уничтожение информации

Подпись: Кража финансовых средств и ценностей. Мошенничество с финансовыми средствами и документами

Подпись: Повреждения зданий, помещений, квартир и другого недвижимого имущества. Вывод из строя средств связи и систем коммунального обслуживания. Кража, угон и уничтожение транспортных средств

Подпись: Моральные и физические страдания:

? убийства

? похищения и угрозы, похищения сотрудников, членов их семей;

? психологичес-кий террор, угрозы, запугивания, шантаж и вымогательство.

Подпись: Информацион-ным ресурсам

Подпись: Финансовым ресурсам

Подпись: Материальным ресурсам

Подпись: Персоналу

Подпись: Внешние

Подпись: Внутренние

Подпись: Угрозы безопасности предприятия. повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности клиентов.

В качестве основных задач системы безопасности рассматриваются:

. своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушению его нормального функционирования и развития; . создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

. пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности; создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей.

Для достижения указанных целей и задач используются различные средства обеспечения безопасности предприятия, среди которых можно выделить следующие [6]:

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

• Организационные средства. Создание специализированных оргструктурных формирований, обеспечивающих безопасность предприятия.

• 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.

• 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.

• Правовые средства. Здесь имеется в виду использование не только изданных вышестоящими органами власти законов и подзаконных актов, но также разработка собственных, так называемых локальных правовых актов по вопросам обеспечения безопасности. • Кадровые средства. Имеется в виду прежде всего достаточность кадров, занимающихся вопросами обеспечения безопасности. Одновременно с этим решают задачи повышения их профессионального мастерства в этой сфере деятельности.

• 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 указанных средств в отдельности не дает необходимого эффекта, он возможен только на комплексной основе, который может быть реализован в виде определенной последовательности следующих 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.

При реализации этих средств используются соответствующие им методы. Соответственно можно говорить о технических, организационных, информационных, финансовых, правовых, кадровых и интеллектуальных методах. Приведем краткий конкретный перечень этих методов:

технические – наблюдение, контроль, идентификация и т.д.;

организационные – создание зон безопасности, режим, расследование, посты, патрули и т.д.;

информационные – сбор сведений о сотрудниках, аналитические материалы и учеты конфиденциального характера и т.д.;

финансовые – материальное стимулирование сотрудников, имеющих достижения в обеспечении безопасности, денежное поощрение информаторов и т.д.;

правовые – судебная защита законных прав и интересов, содействие правоохранительным органам и т.д.;

кадровые – подбор, расстановка и обучение кадров, обеспечивающих безопасность предприятия, их воспитание и т.д.;

интеллектуальные – патентование, ноу-хау и т.д. [6].

1.2. Защита информации в системе безопасности предприятия

При создании систем безопасности на предприятии в последние годы особое внимание уделяется вопросам защиты информации, которая в современном производстве становится одним из главных объектов посягательств и угроз со стороны конкурентов и злоумышленников. Особенно это относится к конфиденциальной информации в наибольшей степени представляющей интерес, например, для конкурирующих фирм. Поэтому наряду с общим понятием безопасности предприятия (БП) рассматривается понятие информационной безопасности.

Информационная безопасность (ИБ) – это состояние защищенности информационной среды предприятия, обеспечивающее его функционирование и развитие в интересах его персонала.

При построении модели информационной безопасности предприятия учитывают целый ряд компонентов (источников, объектов, действий). Наиболее важными среди них являются следующие [12]:

. объекты угроз;

. угрозы;

. источники угроз;

. цели угроз со стороны злоумышленников;

. источники информации;

. способы неправомерного овладения конфиденциальной информацией (способы доступа);

. направления защиты информации;

. способы защиты информации;

. средства защиты информации.

Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов).

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы.

Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба.

Неправомерное овладение конфиденциальной информацией возможно путем ее разглашения источниками сведений, утечки информации через технические средства и несанкционированного доступа к охраняемым сведениям. Учитывая важность этих понятий для дальнейшего изложения материала, рассмотрим их более подробно.

1. Разглашение – это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним [14].

Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией. Реализуется разглашение по формальным и неформальным каналам распространения информации. К формальным коммуникациям относятся деловые встречи, совещания, переговоры и тому подобные формы общения: обмен официальными деловыми и научными документами при помощи средств передачи официальной информации (почта, телефон, телеграф и др.). Неформальные коммуникации включают личное общение (встречи, переписка и др.); выставки, семинары, конференции и другие массовые мероприятия, а также средства массовой информации (печать, газеты, интервью, радио, телевидение и др.). Как правило, причиной разглашения конфиденциальной информации является недостаточное знание сотрудниками правил защиты коммерческих секретов и непонимание (или недопонимание) необходимости их тщательного соблюдения. Тут важно отметить, что субъектом в этом процессе выступает источник (владелец) охраняемых секретов.

Следует отметить информационные особенности этого действия. Информация содержательная, осмысленная, упорядоченная, аргументированная, объемная и доводится зачастую в реальном масштабе времени. Часто имеется возможность диалога. Информация ориентирована в определенной тематической области и документирована. Для получения интересующей злоумышленника информации последний затрачивает практически минимальные усилия и использует простые легальные технические средства (диктофоны, видеомониторинг).

2. Утечка – это бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена [12].

Утечка информации осуществляется по различимым техническим каналам. Известно, что информация вообще переносится или передается либо энергией, либо веществом. Это либо акустическая волна (звук), либо электромагнитное излучение, либо лист бумаги (написанный текст) и др. С учетом этого можно утверждать, что по физической природе возможны следующие пути переноса информации: световые лучи, звуковые волны, электромагнитные волны, материалы и вещества. Соответственно этому классифицируются и каналы утечки информации на визуально-оптические, акустические, электромагнитные и материально-вещественные. Под каналом утечки информации принято понимать физический путь от источника конфиденциальной информации к злоумышленнику, посредством которого последний может получить доступ к охраняемым сведениям. Для образования канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также наличие на стороне злоумышленника соответствующей аппаратуры приема, обработки и фиксации информации.

3. Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам [12].

Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении «продать» секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действии злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения – стационарные или в подвижном варианте, оборудованные самыми современными техническими средствами.

Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников.

Каждая угроза влечет за собой определенный ущерб – моральный или материальный, а защита и противодействие угрозе призвана снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удается далеко не всегда. С учетом этого угрозы могут быть классифицированы по следующим признакам [14]:

• по величине принесенного ущерба:
. предельный, после которого фирма может стать банкротом;
. значительный, но не приводящий к банкротству;
. незначительный, который фирма за какое-то время может компенсировать и др.;

• по вероятности возникновения:
. весьма вероятная угроза;
. вероятная угроза;
. маловероятная угроза;

• по причинам появления:
. стихийные бедствия;
. преднамеренные действия;

• по характеру нанесенного ущерба:
. материальный;
. моральный;

• по характеру воздействиям:
. активные;
. пассивные;

• по отношению к объекту:
. внутренние;
. внешние.

Степень опасности внутренних и внешних угроз может быть проиллюстрирована на примере анализа условий, способствующих неправомерному овладению конфиденциальной информацией [12]:

. разглашение (излишняя болтливость сотрудников) – 32%;

. несанкционированный доступ путем подкупа и склонения к сотрудничеству со стороны конкурентов и преступных группировок – 24%;

. отсутствие в фирме надлежащего контроля и жестких условий обеспечения информационной безопасности – 14%;

. традиционный обмен производственным опытом – 12%;

. бесконтрольное использование информационных систем – 10%

. наличие предпосылок возникновения среди сотрудников конфликтных ситуаций, связанных с отсутствием высокой трудовой дисциплины, психологической несовместимостью, случайным подбором кадров, слабой работой кадров по сплочению коллектива – 8%.

Этот пример убедительно показывает, что одним из основных источников угроз для информационной безопасности является внутренний фактор, на который следует обращать первостепенное внимание при создании соответствующих служб защиты информации.

1.3. Концептуальные модели компонентов системы безопасности предприятия

Концепция выражает систему взглядов на проблему безопасности предприятия на различных этапах и уровнях производственной деятельности, а также основные принципы, направления и этапы реализации мер безопасности. Зарубежный и отечественный опыт обеспечения безопасности свидетельствует, что для борьбы со всей совокупностью преступных и противоправных действий необходима стройная и целенаправленная организация процесса противодействия.

Причем в организации этого процесса должны участвовать профессиональные специалисты, администрация фирмы, сотрудники и пользователи, что и определяет повышенную значимость организационной стороны вопроса.

Накопленный опыт также показывает, что [14]:

. обеспечение безопасности не может быть одноразовым актом. 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 узких мест и потенциальных угроз фирме;

. безопасность может быть обеспечена лишь при комплексном использовании всего арсенала средств защиты и противодействия во всех структурных элементах производственной системы и на всех этапах технологического цикла. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм – СИСТЕМУ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (СБП);

. никакая СБП не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала и пользователей и соблюдения ими всех установленных правил, направленных на обеспечение безопасности.

С учетом накопленного опыта систему безопасности предприятия можно определить как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих безопасность деятельности предприятия от внутренних и внешних угроз.

Учитывая виды угроз, направления и средства защиты личности (персонала) продукции (материальных ценностей) и информации на предприятии В.И. Ярочкиным [13, 14] были предложены концептуальные модели безопасности личности (рис. 1.2.), продукции (рис. 1.3.) и информации (рис. 1.4.).

С учетом этих моделей может быть сформирована общая схема, определяющая содержание и взаимосвязь целей и задач системы безопасности предприятия (рис. 1.5).

Представленная на схеме совокупность целей и задач может рассматриваться в качестве концептуальной модели компонентов СБП.

ЛИЧНОСТЬ
МЕТОДЫ ЗАЩИТЫ
НАПРАВЛЕНИЯ ЗАЩИТЫ
СРЕДСТВА ЗАЩИТЫ
ВРЕМЯ ПОСЯГАТЕЛЬСТВА
ИСТОЧНИКИ УГРОЗУГРОЗЫ
ОБЪЕКТЫ УГРОЗ
МЕСТА ПРЕБЫВАНИЯ

дом, дача рабочий кабинет улица транспорт общественные места самозащита личная охрана юридическая физическая информационная личности кабинета квартиры автомобиля гаража личное рабочее отпуск командировка на жизнь здоровье свободу личное достоинство документы деньги и ценности хулиганы невменяемые (пьяные, наркоманы и др.) преступники убийцы личность члены семьи родственники знакомые имущество убийства насилие грабежи шантаж нападение оскорбления

Подпись: Рис. 1.2. Концептуальная модель безопасности личности

Подпись: Рис. 1.3. Концептуальная модель безопасности продукции
Подпись: Рис. 1.4. Концептуальная модель безопасности информации
Рис. 1.5. Цели и задачи системы безопасности [13]

1.4. Принципы построения системы безопасности предприятия

Опыт разработки и использования систем безопасности на различных предприятиях позволяет сформулировать основные принципы, которые следует учитывать при их построении [13]:

1. Комплексность. Этот принцип предусматривает обеспечение безопасности персонала, материальных, финансовых и информационных ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями.

___AcroPDFMTS___AcroPDFMTS___AcroPDFMTS Подпись:
Выявление Подпись:
Предотвращение Подпись:
Отражение Подпись:
Нейтрализация Подпись:
ПересечениеПодпись:
ЛокализацияПодпись:
Уничтожение AcroPDFMTS AcroPDFMTS AcroPDFMTS AcroPDFMTS AcroPDFMTS

2. Своевременность. Этот принцип ориентирован на упреждающий характер мер обеспечения безопасности на ранних стадиях разработки системы безопасности и прогнозирования обстановки, угроз безопасности, 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 предприятия 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 предпринимательской деятельности, информатизации и защиты информации, частной охранной деятельности, а также других нормативных актов по безопасности с применением всех дозволенных методов обнаружения и пресечения правонарушений

6. Обоснованность. Предлагаемые меры и средства защиты должны реализовываться на современном уровне развития науки и техники, быть обоснованными с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

7. Экономическая целесообразность и сопоставимость. Этот принцип ориентирован на определение возможного ущерба и затрат на обеспечение безопасности (критерий "эффективность – стоимость").

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.

9. Взаимодействие и координация. Предполагает осуществление мер обеспечения безопасности на основе четкого взаимодействия всех заинтересованных подразделений и служб, сторонних специализированных организаций в этой области, координацию их усилий для достижения поставленных целей.

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, накопленного отечественного и зарубежного опыта.

11. Централизация управления. Предполагает самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью системы безопасности.

Особое внимание необходимо уделять принципу комплексности. Для обеспечения безопасности во всем многообразии структурных элементов предприятия, при множестве угроз и способов несанкционированного доступа должны применяться все виды и формы защиты и противодействия в полном объеме. Недопустимо применять отдельные формы или технические средства.

Контрольные вопросы

1. Назовите основные виды угроз безопасности предприятия.
2. Перечислите цель и задачи системы безопасности предприятия.
3. Какие средства используются для обеспечения безопасности предприятия?
4. Дайте определение трем видам правомерного овладения конфиденциальной информацией.
5. Определите в процентах степень опасности внутренних и внешних угроз неправомерному овладению информацией.
6. Какие компоненты входят в состав концептуальной модели безопасности информации?
7. Назовите основные принципы построения системы безопасности предприятия?

. Правовые основы деятельности службы безопасности предприятия

2.1. Организационно-функциональные документы системы безопасности предприятия

В своей деятельности служба безопасности предприятия руководствуется целым рядом нормативно-законодательных документов, постановлений правительства, которые представляются в виде набора практических инструкций, таких как инструкции:

• по организации режима и охраны (для соответствующих структурных подразделений);

• защите коммерческой тайны;

• работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;

• организации хранения дел, содержащих конфиденциальную информацию и по работе архивов, хранящих эту информацию;

• инженерно-технической защите информации (для соответствующих структурных подразделений);

• порядке работы с иностранными представителями и представительствами и другие, а также перечня сведений, составляющих коммерческую тайну.

Наиболее важным документом, регламентирующим деятельность службы безопасности предприятия, является закон РФ «О частной детективной и охранной деятельности в РФ». Этим законом регламентируется, что учредителями службы безопасности не могут быть физические лица, даже имеющие соответствующие лицензии. В соответствии с законом учредителем службы безопасности может быть только одно предприятие.

В законе четко определено, что служба безопасности создается в интересах собственной безопасности учредителя, однако роль службы безопасности в ее обеспечении не определена. Представляется, что служба безопасности предназначена прежде всего для организации защиты от всех видов угроз.

Детализация различных угроз, устранение, пресечение или их нейтрализация входит в компетенцию службы безопасности, должна быть отражена 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 [7].

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 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.

Правовое обеспечение службы защиты информации на конкретном предприятии (фирме, организации) отражается в совокупности учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и защиты информации отражаются в уставе (учредительном договоре) в виде следующих положений:

. предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;

. предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

• создавать организационные структуры по защите конфиденциальной информации;

• издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;

• включать требования по защите информации в договоры по всем видам хозяйственной деятельности;

• требовать защиты интересов предприятия со стороны государственных и судебных инстанций;

• распоряжаться информацией, являющейся собственностью предприятия, с целью извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств производства;

• разработать «Перечень сведений конфиденциальной информации».

Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре, который должен содержать следующие требования:

В разделе «Предмет договора».

Администрация предприятия (в том числе и администрация самостоятельных подразделений) ОБЯЗУЕТСЯ обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации.

Трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации.

Администрация обязана учесть требования защиты конфиденциальной информации в правилах внутреннего распорядка.

В разделе «Кадры. Обеспечение дисциплины труда».

Администрация обязуется:

. нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством.

В разделе «Порядок приема и увольнения рабочих и служащих».

. при поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении;

. администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

В разделе «Основные обязанности рабочих и служащих».

Рабочие и служащие обязаны соблюдать требования нормативных документов по защите конфиденциальной информации предприятия.

В разделе «Основные обязанности администрации».

Администрация предприятия, руководители подразделений обязаны:

обеспечить строгое сохранение конфиденциальной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;

. включить в должностные инструкции и положения обязанности по сохранению конфиденциальной информации;

. неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других организационных и хозяйственных документов по обеспечению экономической и информационной безопасности.

Обязательства конкретного сотрудника, рабочего или служащего по защите информации обязательно должны быть оговорены в трудовом договоре (контракте), при заключении которого трудящийся обязуется выполнять определенные требования, действующие на данном предприятии.

Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора.

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.

Использование договоров о неразглашении тайны - вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена.

Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Далее следует задача не допустить утраты коммерческих секретов.

Реализация правовых норм и актов, ориентированных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права. Для понимания этих важных организационно-правовых форм приведем их определения.

Конфиденциальность – это форма обращения со сведениями, составляющими коммерческую тайну, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.

Договоры – это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.

Обязательство – гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия.

2.2. Виды нормативных документов

Правовые основы деятельности службы безопасности определяются соответствующими положениями конституции РФ, а также целым комплексом законов, указов и постановлений правительства.

Ниже рассмотрены наиболее важные из них.

Законы

• Закон РФ от 22 марта 1991г. N 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках» определяет организационные и правовые основы предупреждения, ограничения и пресечения монополистической деятельности и недобросовестной конкуренции и направлен на обеспечение условий для создания и эффективного функционирования товарных рынков.

• Закон РФ от 5 марта 1992г. N 2446-1 «О безопасности» закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

• Закон РФ от 11 марта 1992г. N 2487-1 «О частной детективной и охранной деятельности в Российской Федерации».

• Закон РФ от 23 сентября 1992 г. N 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных».

• Закон РФ от 19 февраля 1993г. N 4524-1 «О федеральных органах правительственной связи и информации».

• Закон РФ от 10 июня 1993 года N 5151-1 «О сертификации продукции и услуг» устанавливает правовые основы обязательной и добровольной сертификации продукции, услуг и иных объектов в Российской Федерации, а также права, обязанности и ответственность участников сертификации.

• Закон РФ от 10 июня 1993 года N 5154-1 «О стандартизации» устанавливает правовые основы стандартизации в Российской Федерации, обязательные для всех государственных органов управления, а также предприятий и предпринимателей, общественных объединений, и определяет меры государственной защиты интересов потребителей и государства посредством разработки и применения нормативных документов по стандартизации.

• Закон РФ от 21 июля 1993 года N 5485-1 «О государственной тайне» регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

• Закон РФ от 20 января 1995 года N 15-ФЗ «О связи» устанавливает правовую основу деятельности в области связи, осуществляемой под юрисдикцией Российской Федерацией, определяет полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи.

• Закон РФ от 20 февраля 1995г. N 24-ФЗ «Об информации, информатизации и защите информации» регулирует отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации, создании и использовании информационных технологий и средств их обеспечения, защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

• Закон РФ от 03 апреля 1995г. N 40-ФЗ «Об органах Федеральной службы безопасности в Российской Федерации» определяет назначение, правовые основы, принципы, направления деятельности, полномочия, силы и средства органов Федеральной службы безопасности, а также порядок контроля и надзора за их деятельностью.

• Федеральный закон от 12 августа 1995г. N 144-ФЗ «Об оперативно-розыскной деятельности» определяет содержание оперативно-розыскной деятельности, осуществляемой на территории Российской Федерации, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий.

• Закон РФ от 4 июля 1996 года N 85-ФЗ «Об участии в международном информационном обмене».

• Федеральный закон от 13 декабря 1996г. N 150-ФЗ «Об оружии» регулирует правоотношения, возникающие при обороте гражданского, служебного, а также боевого ручного стрелкового и холодного оружия на территории Российской Федерации, направлен на защиту жизни и здоровья граждан, собственности, обеспечение общественной безопасности, охрану природы и природных ресурсов, укрепление международного сотрудничества в борьбе с преступностью и незаконным распространением оружия. Положения настоящего федерального закона распространяются также на оборот боеприпасов и патронов к оружию.

• Федеральный закон от 25 сентября 1998г. N 158-ФЗ «О лицензировании отдельных видов деятельности» регулирует отношения, возникающие в связи с осуществлением лицензирования отдельных видов деятельности, и направлен на обеспечение единой государственной политики при осуществлении лицензирования, при регулировании и защите прав граждан, защите их законных интересов, нравственности и

здоровья, обеспечении обороны страны и безопасности государства, а также на установление правовых основ единого рынка.

• Закон РФ от 10 января 2002 года N 1-ФЗ «Об электронной цифровой подписи» определяет правила использования электронной подписи в электронных документах, которая признается равноподлинной собственноручной подписью на бумажном носителе.

Постановления

• Постановление Правительства РФ от 24 декабря 1994 г. N 1418 «О лицензировании отдельных видов деятельности».

• Постановление Правительства РФ от 15 апреля 1995 года N 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и(или) оказанием услуг по защите государственной тайны».

• Постановление Правительства РФ от 26 июня 1995г. N 608 «О сертификации средств защиты информации».

• Постановление Правительства РФ от 04 сентября 1995г. N 870 «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности».

Указы

• Указ Президента РФ от 31 декабря 1993г. N 2334 «О дополнительных гарантиях прав граждан на информацию».

• Указ Президента РФ от 20 января 1994г. N 170 «Об основах государственной политики в сфере информатизации».

• Указ Президента РФ от 3 апреля 1995г. N 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации».

• Указ Президента РФ от 30 ноября 1995г. N 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».

• Указ Президента РФ от 6 марта 1997г. N 188 «Об утверждении перечня сведений конфиденциального характера».

• Указ Президента РФ от 30 мая 1997 года N 226-рп «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне».

Доктрины

Доктрина информационной безопасности РФ (утверждена президентом РФ 9 октября 2000 года) представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации, служит основой для:

. формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;

. подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;

. разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Настоящая доктрина развивает концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

2.3. Лицензирование видов деятельности службы безопасности предприятия

В соответствии с Федеральным законом «О лицензировании отдельных видов деятельности» от 8.08.2001 года №128–ФЗ деятельность различных подразделений службы безопасности предприятия подпадает под требования этого закона, по которому подлежит лицензированию (при наличии этих видов деятельности):

. предоставление услуг в области шифрования информации;

. деятельность:

• по выявлению электронных устройств, предназначенных для негласного получения информации;

• разработке и производству средств защиты конфиденциальной информации;

• технической защите конфиденциальной информации;

• предупреждению и тушению пожаров;

. разработка, производство и приобретение с целью продажи спецсредств для негласного получения информации;

. негосударственная (частная) охранная и сыскная деятельность.

Под лицензией понимается специальное разрешение на осуществление конкретного вида деятельности при обязательном соблюдении лицензионных требований и условий, выданное лицензирующим органом юридическому или физическому лицу.

Лицензирование – процесс, связанный с предоставлением лицензий, переоформлением документов, подтверждающих наличие лицензии, приостановлением, возобновлением или контролем лицензирующих органов за соблюдением правил выполнения лицензионных видов деятельности.

Срок действия лицензии не может быть менее чем 5 лет, в отдельных случаях предусматривается бессрочное действие лицензии.

Существует определенный порядок принятия решения о предоставлении лицензии, которая может быть выдана лицензирующим органом на основании следующих документов:

. заявление о предоставлении лицензии;

. копии учредительных документов и копии свидетельства о госрегистрации;

. копии свидетельства о постановке на учет в налоговом органе;

. документ, подтверждающий уплату лицензионного сбора.

Дополнительные условия и правила лицензирования существуют при получении разрешений определенных видов деятельности в области защиты информации (решение Гостехкомиссии и ФАПСИ от 27.04.94г. №10) и деятельности по технической защите конфиденциальной информации (Постановление Правительства РФ 30.04.02г. №290).

Эту систему лицензирования организуют государственные органы по лицензированию, которыми являются Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) и Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

Государственные органы по лицензированию в пределах их компетенции, установленной законодательством Российской Федерации, осуществляют лицензирование деятельности предприятия в области защиты информации в соответствии с существующими перечнями видов деятельности.

Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию Гостехкомиссией России

1. Сертификация, сертификационные испытания защищенных технических средств обработки информации (ТСОИ), технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств по требованиям безопасности,

программных средств защиты информации, программных средств контроля защищенности информации.

2. Аттестация систем информатизации, автоматизированных систем управления, систем связи и передачи данных, технических средств приема, передачи и обработки подлежащей защите информации, технических средств и систем, не обрабатывающих эту информацию, но размещенных в помещениях, где она обрабатывается (циркулирует), а также помещений, предназначенных для ведения переговоров, содержащих охраняемые сведения, на соответствие требованиям руководящих и нормативных документов по безопасности информации и контроль защищенности информации в этих системах, технических средствах и помещениях.

3. Разработка, производство, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание защищенных ТСОИ, технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств защиты информации, программных средств контроля защищенности информации.

4. Проектирование объектов в защищенном исполнении.

5. Подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне.

Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию ФАПСИ

1. Разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка и ремонт шифровальных средств, предназначенных для криптографической защиты информации при ее обработке, хранении и передаче по каналам связи, а также предоставление услуг по шифрованию информации.

2. Эксплуатация государственными предприятиями шифровальных средств, предназначенных для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

3. Разработка, производство, проведение сертификационных испытаний, реализация, монтаж, наладка, установка, ремонт, сервисное обслуживание специализированных защищенных ТСОИ, технических средств защиты информации, технических средств контроля эффективности мер защиты информации, защищенных программных средств обработки информации, программных средств защиты информации, программных средств контроля защищенности информации, предназначенных для использования в высших органах.

4. Подготовка и переподготовка кадров в области защиты информации по видам деятельности, перечисленным в данном перечне.

Лицензия на право деятельности по защите информации (далее - лицензия) выдается предприятию государственным органом по лицензированию по представлению органа государственной власти Российской Федерации на конкретные виды деятельности на три года, по истечении которых осуществляется ее перерегистрация в порядке, установленном для выдачи лицензии.

Лицензия выдается подавшему заявку на ее получение предприятию-заявителю, располагающему производственной и испытательной базой, нормативной и методической документацией, научным и инженерно-техническим персоналом, при условии их соответствия требованиям государственного органа по лицензированию на основании результатов экспертизы деятельности предприятия по заявленному направлению работ. С этими требованиями заявитель имеет право ознакомиться в государственном органе по лицензированию.

Для получения лицензии в этом случае представляется расширенный комплект документов: заявление; представление органа государственной власти Российской Федерации; материалы экспертизы, подтверждающие наличие необходимых условий для

проведения работ по заявленным видам деятельности, а также профессиональную пригодность руководителя предприятия-заявителя или лиц, уполномоченных им для руководства лицензируемой деятельностью; копии документов о государственной регистрации предпринимательской деятельности и устава предприятия.

Отказ в выдаче лицензии производится в случаях, если отсутствуют необходимые условия для проведения работ по заявленному виду деятельности; профессиональная подготовка руководителя предприятия-заявителя, или лиц, уполномоченных им для руководства лицензируемой деятельностью, не соответствует установленным требованиям; в представленных для получения лицензии документах указаны недостоверные сведения; заявитель в установленном законом порядке признан виновным в недобросовестной конкуренции в лицензируемой деятельности.

2.4. Рекомендации по разработке уставных документов службы безопасности предприятия

Несмотря на большое количество законодательных актов, регламентирующих деятельность в сфере обеспечения безопасности предприятий, во многих случаях при практической деятельности работники СБП сталкиваются с их противоречиями, например при оказании платных услуг другим предприятиям и физическим лицам, при использовании определенных видов оружия в охранной деятельности и др.

В определенной мере этот провал можно преодолеть путем тщательной правовой обработки устава службы безопасности.

Уставом называется правовой акт, определяющий свод правил, регулирующих деятельность организации, ее взаимоотношения с другими организациями и гражданами, права и обязанности в определенной сфере ее деятельности.

Рассмотрим для примера типовой устав службы безопасности, предложенный В.П. Мак-Маком [7], на основе которого путем конкретизации с учетом особенностей предприятия можно подготовить индивидуальный устав.

Сложность в разработке устава заключается в том, что в нем должны быть изложены в краткой, но емкой форме, основы жизнедеятельности службы безопасности. Исходя из общих требований к уставам организаций, в него целесообразно включить следующие разделы:

I. Общие положения. II. Основные задачи. III. Функции. IV. Права и обязанности. V. Руководство. VI. Взаимоотношения и связи. VII. Охранная и детективная деятельность. VIII. Имущество и средства. IX. Контроль, проверка и ревизия деятельности. X. Реорганизация и ликвидация [7].

Раздел «Общие положения» содержит перечень нормативных актов, которыми должны руководствоваться в своей деятельности сотрудники службы безопасности; полное наименование и адрес местонахождения предприятия-учредителя: название документа, на основании которого создается служба безопасности (протокол, приказ, решение коллегии и т.д.), и дату его учреждения; место службы безопасности и его подчиненность в структуре предприятия: деятельность службы безопасности, принципы деятельности; наличие текущего, расчетного счета: порядок финансирования. Чрезвычайно большое значение имеет формулирование цели деятельности службы безопасности, так как именно от этого зависит, какие задачи и функции будут поставлены перед ней. Анализ закона, других нормативных актов и литературы позволяет определять цель деятельности службы безопасности как своевременное пресечение (нейтрализацию) противоправных посягательств на экономические интересы и персонал предприятия. Следует при этом учитывать, что цель деятельности службы безопасности определяет руководитель предприятия-учредителя, поэтому возможны и другие его формулировки.

Среди принципов деятельности выделим такие, как соблюдение законности, эффективность и конфиденциальность, выполнение общепризнанных этических норм, плановость, защита законных интересов учредителя.

Раздел «Основные задачи» включает те задачи, выполнение которых возможно в рамках предоставленной службе безопасности компетенции, и реализация которых приведет к достижению обозначенной цели. Применительно к приведенной нами цели основные задачи можно сформулировать следующим образом:

. охрана собственности и защита персонала от противоправных посягательств;

. координация действий сотрудников и структур предприятия по вопросам обеспечения безопасности;

. содействие правоохранительным органам и судам по вопросам, затрагивающим интересы предприятия;

. защита от несанкционированного доступа к закрытой информации о персонале и деятельности предприятия;

. сбор, обработка и анализ конфиденциальной информации среди персонала предприятия и в сфере предпринимательства.

Раздел «Функции» включает перечень функций и составляется с учетом того, что их выполнение позволит реализовать ранее обозначенные основные задачи. Сами функции можно разделить на группы: внешние и внутренние. К внешним функциям относятся те из них, которые названы в законе видами предоставляемых услуг:

• обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий;

• консультирование и предоставление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности;

• охрана имущества предприятий;

• защита жизни и здоровья персонала от противоправных посягательств;

• сбор информации для проведения деловых переговоров;

• изучение криминальных аспектов рынка:

• выявление ненадежных деловых партнеров:

• сбор сведений по гражданским делам:

• розыск без вести пропавших сотрудников предприятия;

• выявление некредитоспособных партнеров;

• поиск утраченного имущества предприятия;

• расследование фактов неправомерного использования товарных (фирменных) знаков предприятия;

• сбор информации о лицах, заключавших с предприятием контракты;

• расследование фактов разглашения коммерческой тайны предприятия;

• сбор сведений по уголовным делам;

• установление обстоятельств недобросовестной конкуренции со стороны других предприятий;

• проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации.

Что касается разработки внутренних функций, то здесь никаких ограничений не существует. Можно лишь рекомендовать тот минимум функций, отсутствие которых негативным образом скажется на эффективности деятельности службы безопасности. К ним, в частности, относятся анализ состояния безопасности предприятия, планирование деятельности по обеспечению этой безопасности, координация деятельности и организация взаимодействия между подразделениями службы безопасности и предприятия, ресурсное (кадровое, финансовое, материально-техническое и т.д.) обеспечение, контроль и проверка деятельности, оценка эффективности деятельности СБ и предприятия по вопросам безопасности.

Раздел «Права и обязанности» рассматривает права и обязанности сотрудников подразделений СБП, включающих такие, как внесение предложений руководству и структурным подразделениям предприятия, контроль за соблюдением режима безопасности, проведение расследований, изменение структуры службы безопасности, осуществление взаимодействия с правоохранительными и контрольно-надзорными органами, распоряжение предоставленными финансовыми средствами по своему усмотрению, в некоторых случаях запрета проведения определенных работ, самостоятельный набор и увольнение своих сотрудников и т.д.

Раздел «Руководство» определяет подчиненность начальника службы безопасности одному из руководителей предприятия, порядок выполнения распоряжений руководителя предприятия-учредителя, обязанности персонала выполнять указания руководителей службы безопасности и процедуру обжалования их неправомерных действий, порядок назначения и освобождения руководителей службы безопасности, перечень основных квалифицированных требований к ним, ответственность и т.д.

Раздел «Взаимоотношения и связи» регламентирует процедуры контактов СБ с руководителями и конкретными подразделениями предприятия, правоохранительными, контрольно-надзорными и судебными органами, средствами массовой информации, деловыми партнерами учредителя, депутатским корпусом и т.д.

Раздел «Охранная и детективная деятельность» отражает такие вопросы, как наименование оргструктурных формирований, занимающихся сыскной и охранной деятельностью, методы и средства, применяемые сотрудниками СБ, ограничения в охранной и детективной деятельности, обязательность регулирования деятельности сотрудников СБ внутренними нормативными актами (положения об отделах, должностные инструкции и т.д.), критерии оценки деятельности службы безопасности и т.д.

Раздел «Имущество и средства» описывает перечень необходимых для функционирования службы безопасности мебели, компьютеров, автомашин, средств связи, помещений, спецсредств и оружия, форменного обмундирования и т.д. (без указания потребного их количества). Кроме материально-технических средств, в этот перечень рекомендуется включить условия и порядок финансирования службы безопасности и её сотрудников, наличие компьютерных программ, специальной литературы и нормативных актов и т.д.

Раздел «Контроль, проверка и ревизия деятельности» определяет субъектов этой деятельности, их правомочия, порядок доступа к документации службы безопасности, место и время хранения контрольных документов, формы и методы устранения выявленных недостатков.

Раздел «Реорганизация и ликвидация» фиксирует основания и порядок реорганизации и ликвидации службы безопасности, необходимость создания ликвидационной комиссии, сохранения социальных гарантий в отношении увольняемых сотрудников и т.д.

Проект Устава службы безопасности подписывается его начальником, утверждается руководителем предприятия-учредителя и представляется на согласование начальнику органа внутренних дел района.

К разработке проекта следует относиться внимательно и квалифицированно, так как от качества этого проекта в дальнейшем во многом зависит эффективность деятельности службы безопасности.

В прил. 1 приведен пример устава службы безопасности предприятия, разработанный в соответствии с рассмотренными рекомендациями.

Контрольные вопросы

1. Какими инструкциями руководствуются при организации работы службы безопасности предприятия?
2. Назвать основные виды безопасности на предприятии.
3. Что необходимо включать в коллективный договор для правового обеспечения защиты информации?
4. Перечислить основные нормативные документы, регламентирующие деятельность в области защиты информации.
5. В чем состоит суть лицензирования деятельности предприятий в области защиты информации?
6. Какие виды деятельности предприятия в области защиты информации необходимо лицензировать?
7. Назвать разделы устава службы безопасности предприятии и дать им характеристику.

Глава 3. Организационное проектирование деятельности службы безопасности предприятия

3.1. Основы организационного проектирования систем управления

Система управления СБП может быть рассмотрена с позиции общего подхода к построению социальных организационных систем. В этом случае выделяется три вида управленческой деятельности:

1. Стратегическое управление – анализ и прогноз динамики внешней и внутренней ситуации на предприятии, определение целей организационных структур службы безопасности, выявление проблем на пути достижения основной цели; разработка возможных вариантов поэтапного достижения цели, оценка рисков и экономического обоснования.
2. Текущее (календарное) управление – разработка основных технологий организации систем безопасности предприятия, организация взаимодействия всех подразделений службы безопасности, разработка оперативных планов реализации отдельных этапов выбранного варианта стратегической программы.
3. Оперативное регулирование (руководство) – управление воздействиями на персонал СБП и всего предприятия с целью предотвращения угроз безопасности предприятия.

При разработке систем управления СБП обычно не удается использовать типовые организационные структуры, схемы структурных и функциональных регламентов отдельных подразделений, что связано с неповторяемостью рассматриваемых ситуаций в области защиты информации на конкретном предприятии. Учитывая это обстоятельство при создании службы безопасности предприятия и входящей в его состав службы защиты информации используются новые подходы, основанные на использовании методики организационного и организационно-кадрового проектирования систем управления, позволяющих учитывать конкретные условия, для которых создается СБП.

Наиболее известна в этом направлении работа В.С. Соловьева «Организационное проектирование систем управления» [8], на основе которой ниже рассмотрены общие методы к решению рассматриваемой проблемы.

Система управления, как и любая система деятельности, состоящая из функционально взаимодействующих элементов, представляет собой совокупность материальных, технических, кадровых, информационных, финансовых ресурсов и организационных условий деятельности, обеспечивающих ее целостность. При рассмотрении системы управления как объекта проектирования рекомендуется выделять ряд функциональных элементов – объектов организационного проектирования [8]:

• Субъекты управленческой деятельности: управленческие работники (управленческий персонал, кадры), описываемые в системе управления в качестве функциональных должностных позиций (с выделением позиций высшего управленческого персонала и руководителей) и реализуемые в форме организационной структуры системы управления как обособленного аппарата (органа) управления.

• Средства управленческой деятельности в форме нормативно-справочной и инструктивно-методической информации.

• Предмет управленческой деятельности, выступающей в форме информации, используемой для выработки управленческих решений, материальных ресурсов для предоставления информации (бумага, числовые носители информации и т.п.).

• Производственно-бытовые и организационно-экономические условия деятельности: административные здания, помещения, мебель, санитарно-гигиенические условия труда, техника безопасности, пространственное размещение и оборудование рабочих мест, система оплаты труда и т.п.

• Результат, содержание управленческой деятельности, отражающие динамику состояний всех элементов производственно-хозяйственной деятельности и предоставляемые в форме документированных организационно-распорядительных, проектно-технологических, планово-экономических управленческих решений.

Под организационным проектированием понимается разработка проекта системы управления и основных элементов (техники управления, организационных условий управленческой деятельности) в виде комплекса формализованных документов, описывающих информационные (документальные) функциональные взаимосвязи (содержательные) и административные связи (подчинения) в структуре функциональных подсистем, должностных позиций и подразделений системы управления [8].

В современном понимании организационное проектирование включает решение трех основных задач:

1) проектирование функциональной управленческой деятельности;

2) организационно-кадровое проектирование;

3) кадровое проектирование стратегического управления и руководства.

Общее содержание, структура и порядок организационного проектирования систем управления, включающий три рассмотренные задачи, может быть показан в виде схемы (рис.3.1.).

Содержание управленческой деятельности, структура системы управления и численность аппарата управления обусловливаются прежде всего целями организации и соответственно задачами, которые должна решать система управления для достижения этих целей.

Рис 3.1. Принципиальная схема организационного проектирования систем управления

Подпись: 13. Разработка рабочей документации организационного проекта

Подпись: 12.Формирование организационной структуры системы управления

Подпись: 11.Разработка содержания нефункциональной творческой управленческой деятельности

Подпись: 7.Описание внутриорганизационного объекта управления

Подпись: 5.Декомпозиция цели организации по элементам производственных процессов и организационным условиям деятельности

Подпись: 9.Расчет численности управленческого персонала и разработка структуры функциональной управленческой деятельности

Подпись: 6.Формулировка задач системы управления

Подпись: 1.Анализ динамики внутреннего состояния организации

Подпись: 10.Описание внешнего объекта управления

Подпись: 3.Анализ и прогноз динамики внешней ситуации

Подпись: 4.Определение цели организации (целевых производственно-экономических параметров организации)

Подпись: 8.Проектирование содержания функциональной управленческой деятельности

Подпись: 2.Организационно-функциональный и кадровый анализ системы управления действующих организаций.

В связи с тем, что содержание управленческой деятельности обусловлено прежде всего особенностями определенных видов деятельности СБП, разработка организационного проекта системы управления создаваемой организации должна начинаться тогда, когда есть технический проект (ТП) или технорабочий проект (ТРП) организации предприятия и его соответствующих служб. В наиболее общем виде процесс организационного проектирования может быть представлен в виде 15 этапов.

Данные этапа 1 (рис.3.1.), характеризующие производственно-хозяйственную деятельность организации, являются информационной основой для анализа и прогноза внешней ситуации, так как именно по этим элементам и этапам их «жизненных циклов» проводится анализ и дается прогноз внешней ситуации.

На основе анализа и прогноза динамики внешней ситуации с точки зрения экономического, кадрового, социального и криминального состояния региона, страны и международной ситуации устанавливается цель организации создаваемой службы (этапы 2, 3), которая затем декомпозируется во внутриорганизационные цели и задачи системы управления СБП по всем элементам и этапам «жизненных циклов» этих элементов, осуществляемых в рамках организации и собственно представляющих целевые характеристики содержания внутриорганизационной управленческой деятельности (этапы 4.5).

Одновременно с этим формулируются цели и задачи системы управления, реализуемые во внешней среде (этап 6).

На основании сформулированных целей и задач системы управления и состояния внутриорганизационного объема (этап 7) проектируется содержание управленческой деятельности (этап 8) и определяется необходимая численность аппарата управления (этап 9).

Содержание и объем функциональной управленческой деятельности определяются на основании разработки функциональных задач и соответствующего проектирования системы документов и технического обеспечения управленческой деятельности. Методика проектирования функционального содержания управленческой деятельности и информационного документального обеспечения рассмотрена ниже.

Заключительным этапом организационного проектирования, когда решаются основные принципиальные вопросы формирования и функционирования системы управления, является разработка структуры системы управления (этап 12). На этом этапе окончательно устанавливается организационная структура (управленческая и производственная структуры организации), определяются состав и структура высшего управленческого персонала, информационного и технического обеспечения управленческой деятельности, схемы документооборота и информационных взаимосвязей, распределения полномочий и ответственности управленческого персонала.

Методика проектирования организационной структуры системы управления также приводится ниже.

Завершается организационное проектирование системы управления СБП расчетом экономической эффективности проектных решений и разработкой рабочей документации организационного проекта (этап 13), в состав которого входят положения об основных структурных подразделениях службы безопасности предприятия, должностные инструкции, схемы организации рабочих мест, проект технического оснащения системы управления, рабочие формы документов и т.п.

3.2. Методика проектирования функционального содержания управленческой деятельности

На основании декомпозиции целей и определения функциональных задач системы управления, о чем излагалось выше, проектируется содержание функциональной управленческой деятельности.

Принципиальная схема такого проектирования дана на рис.3.2.

Любая организация представляет собой социально-экономическую специализированную систему различных видов деятельности. В свою очередь, деятельность как элемент организации – это сложное системное образование, включающее субъект, предмет, средства, условия, результат деятельности и процесс деятельности как последовательную смену структурированных состояний всех элементов деятельности.

Рис.3.2. Принципиальная схема проектирования содержания функциональной управленческой деятельности

Поэтому, чтобы организовать и осуществить совместную деятельность, необходимо ее предварительно мысленно представить и описать (зафиксировать) в абстрактной форме каких-либо знаковых систем, т.е. деятельность может быть реализована как разумная и сознательная только в том случае, когда она формально предварительно описана. Формализованное описание производственной деятельности составляет содержательную сущность управления, т.е. управленческой деятельности [8].

Подпись: Проект технического обеспечения системы управления

Подпись: Макеты рабочих форм документов

Подпись: 5.Проектирование информационного обеспечения системы управления

Подпись: 7.Определение нормативной трудоемкости документальных операций

Подпись: 4.Формирование предварительного перечня документов, обеспечивающих выполнение специфических функций управления

Подпись: 6.Определение операционального содержания функциональной управленческой деятельности

Подпись: 9.Определение нормативной численности функционального управленческого персонала

Подпись: 8.Нормативное проектирование функциональной управленческой деятельности

Подпись: Классификатор функциональной управленческой деятельности

Подпись: 3.Определение состава специфических функций и задач управления, осуществляемых в организации

Подпись: 2.Определение стадий «жизненных циклов» элементов организации, осуществляемых внутри организации

Подпись: 1.Определение состава общих функций управления, осуществляемых в организации

3.3. Методика проектирования организационной структуры системы управления

Под организационной структурой, или структурой организации в целом, понимается схема иерархически упорядоченной совокупности подразделений организации и их административных взаимосвязей подчинения, субординации, обеспечивающих целостность организации как социально-экономической специализированной системы различных видов деятельности. Структура организации является её основной статической характеристикой, определяющей, с одной стороны, потенциальную устойчивость и стабильность существования – функционирования организации как системы, а с другой стороны - консервативную неадекватность статического состояния организации в условиях постоянной динамики объективного мира. Прежде всего, в структуре деятельностных организаций можно выделить две взаимосвязанные подсистемы: производственную и управляющую.

Производственная подсистема предопределяет достижение основной цели соответствующей организации, а управляющая подсистема обеспечивает социально-экономическую целесообразную ее реализацию. Соответственно такому делению организации как системы можно говорить о СБП как о совокупности организационной и управленческой составляющей. Первая представляет собой состав и взаимосвязи исполнительных подразделений, вторая – соответственно состав и взаимосвязи управленческих подразделений и должностных позиций.

Таким образом, под организационной структурой СБП можно понимать состав территориально (пространственно) обособленных, специализированных по определенным направлениям деятельности, производственных подразделений организации и организационно-технологические связи между этими подразделениями.

Под подразделением (отделом) в рамках СБП в дальнейшем будет пониматься такое структурное объединение, численность которого составляет более трех человек, из которых один - начальник отдела.

Необходимо отметить, что когда речь заходит об организационных структурах систем управления, всегда встает вопрос о характере взаимосвязей элементов этих систем. В отличие от расчетных технико-технологических описаний физических, материально-вещественных функциональных взаимосвязей в процессах производственной деятельности, в системе управленческой деятельности связи информационные, абстрактные носят идеальный характер. Как правило, в научной литературе по управлению различают два вида связей в организациях: линейные и функциональные. Соответственно этому организационные структуры систем управления обозначаются как линейные, функциональные, а также различные виды комбинированных, линейно-функциональных структур [8].

Понятием «линейные связи» обозначают организационно-управленческие административные связи подчинения. В подавляющем большинстве литературных источников по теории управления линейные связи рассматривают как чисто властные «командные» авторитарные взаимоотношения. Однако это далеко не так. Любые властные воздействия, даже в жесткой форме приказов, обязательно предполагают содержательный контекст, иначе управление может вообще не состояться, так как основа управленческой деятельности – ясность и понимание того, что необходимо сделать. Поэтому в линейных связях, наряду с властным компонентом, обязательно должно содержаться функциональное (регламентированное) содержание. Более того, основой линейных связей управления, безусловно, является, прежде всего, смысловое содержание, но выраженное во властной форме. Термин линейный означает лишь то, что все виды отношений между управляющими и исполняющими элементами организации, с одной стороны, реализуются как связи непосредственного административного подчинения, а с другой стороны, осуществляются по одной «линии», по одному информационному «каналу».

Под функциональными связями элементов любой системно организованной деятельности необходимо понимать жестко регламентированные, нормированные, кооперативно-последовательные зависимости одних элементов от других. Функциональные связи предполагают операциональное описание технологии выполнения управленческой деятельности, т.е. описывают последовательность выполнения операций и собственно сами способы, операции или отдельные приемы и действия. Таким образом, содержание любой кооперированной деятельности формально может быть описано через технологическую структуру операциональных функциональных взаимосвязей элементов организации. Именно это позволяет структурировать функциональную управленческую деятельность по отдельным функциональным подразделениям и должностным позициям [8].

Все инструктивно-методические рекомендации, функциональные должностные инструкции, составленные специалистами, приобретают силу нормативного документа, обязательного для исполнения, только после их утверждения высшим административным управленческим персоналом. Таким образом, функциональные взаимосвязи реализуются через структуру административных связей подчинения. Следовательно, все схемы организационных структур систем управления, хотя и отражают только линейные административные связи подчинения, являются по существу линейно-функциональными структурами одного типа.

При проектировании организационной структуры используется метод нормативного проектирования, в основе которого лежит расчет численности управленческого персонала на основе определения трудоемкости отдельных видов функциональной управленческой деятельности. Состав, структура этапов и последовательность нормативного проектирования организационной структуры системы управления приведена на рис.3.3.

Трудоемкость функциональной управленческой деятельности включает трудоемкость разработки документов и трудоемкость решения организационных вопросов.

3.4. Методика оформления основных документов организационного проекта системы управления

Важным этапом организационного проектирования является разработка комплекта документов, регламентирующих состав, функции и взаимосвязь организационных структур.

В состав рабочей документации организационного проекта системы управления включаются следующие документы [8]:

• схема организационной структуры системы управления;

Подпись: 13. Разработка рабочей документации организационного проекта

• схема документооборота;

• схемы информационных связей;

• рабочие формы управленческой документации;

• положения о функциональных структурных подразделениях системы управления;

• должностные инструкции работникам системы управления.

Рис.3.3. Принципиальная схема проектирования организационной структуры системы управления [8]

Подпись: 9.Разработка линейных карт распределения полномочий (обязанностей)

Подпись: 10.Разработка схем документооборота и схем информационных связей

Подпись: 11.Разработка положений об отделах и должностных инструкциях по основным рабочим местам в системе управления

Подпись: Проект технического обеспечения системы управления

Подпись: Технический проект организации

Подпись: 8.Формирвоание уровня централизации принятия решений

Подпись: 7.Разработка схемы организационной структуры

Подпись: 6.Формирование зон управляемости высшего управленческого персонала

Подпись: 5.Формирование функциональной структуры управления

Подпись: 4.Определение численности и формирование состава функциональных структурных подразделений

Подпись: 3.Определение трудоемкости и численности по основным функциональным подсистемам

Подпись: 2.Расчет общей численности функционального управленческого персонала

Подпись: 1.Расчет (определение) трудоемкости разработки документов и организационных видов деятельности

Схема организационной структуры системы управления составляется в соответствии с требованиями, рассмотренными выше. В ней отражаются все функциональные структурные управленческие и производственные подразделения, должностные позиции высшего управленческого персонала и организационные взаимосвязи непосредственного подчинения.

В дополнение к общей схеме организационной структуры системы управления могут разрабатываться схемы организационной структуры отдельных функциональных подразделений (отделов и служб). Пример оформления схемы организационной структуры общего отдела приведен на рис.3.4.

Рис.3.4. Принципиальная схема организационной структуры функционального отдела системы управления

Схема документооборота определяет установленный организационным проектом порядок прохождения документов между функциональными подразделениями и высшим управленческим аппаратом системы управления. Для этого используются специальные схемы, отражающие последовательность прохождения документов между подразделениями.

Аналогичные схемы строятся для отображения информационных связей между подразделениями внутри СБП.

Подпись: Инженер

Подпись: Инженер

Подпись: Гл. специалист

Подпись: Рук. Группы

Подпись: Инженер

Подпись: Заместитель начальника отдела

Подпись: Ст. инженер

Подпись: Ст. инженер

Подпись: Гл. специалист

Подпись: Начальник отдела

Рабочие формы управленческой документации разрабатываются в соответствии с требованиями стандартов ЕОКД, ЕСТПП, ЕСГД и др. Состав реквизитов, показателей и параметров отдельных документов принимается на основании результатов проектных решений, полученных при разработке информационного обеспечения системы управления.

Особое внимание при детализационном проектировании деятельности СБП уделяется вопросам разработки положений о структурных подразделениях и должностным инструкциям работников СБП.

Положения о функциональных структурных подразделениях разрабатываются на основании параметров организационного проекта по результатам всех стадий организационного проектирования систем управления. Положения должны иметь следующую типовую структуру:

Титульный лист

1. Общая часть
2. Организационная структура
3. Функциональные задачи
4. Права и ответственность начальника функционального подразделения

На титульном листе указываются основные реквизиты подразделения: полное и сокращенное наименование функционального структурного подразделения, срок ввода в действие и длительность действия положения, подпись, дата, должность, фамилия, имя и отчество лица, утвердившего положение. Наличие всех указанных реквизитов придает документу юридическую силу.

В разделе 1 «Общая часть» указываются место и назначение функционального структурного подразделения в системе управления, кому непосредственно подчиняется подразделение в структуре управления, порядок его создания, переформирования и ликвидации (кто решает, когда и при каких условиях изменяются состав, структура и назначение), какими нормативными актами руководствуется отдел в своей работе (какие нормативные акты определяют сферу деятельности и ответственность отдела). В общей части может быть указан порядок назначения, перемещения и увольнения начальника функционального подразделения.

В разделе 2 «Организационная структура функционального структурного подразделения» указываются схема организационной структуры и распределение функциональных задач по должностным позициям. В этом разделе может быть приведено также штатное расписание функционального подразделения.

В разделе 3 «Функциональные задачи» указывается; перечень функциональных задач и операций, выполняемых отделом.

В разделе 4 «Права и ответственность начальника функционального подразделения» указываются права, необходимые отделу для выполнения функциональных задач, и ответственность за их выполнение. Права и ответственность устанавливаются в полном соответствии с функциональными задачами и обязанностями функционального подразделения. Для сокращения объема данного раздела одинаковые права, необходимые для выполнения различных функциональных задач, и одинаковая ответственность за выполнение функциональных задач могут быть сгруппированы. Нужно четко выделить различные виды и степень ответственности функциональных задач, которые должны решаться на данной должности.

Должностные инструкции работникам системы управления разрабатываются также с учетом определенных требований и должны состоять из следующих разделов:

Титульный лист

1. Общие положения
2. Квалификационные требования
3. Функциональные обязанности
4. Права
5. Ответственность

Титульный лист содержит все необходимые реквизиты, обеспечивающие юридическую силу документа: полное наименование функциональной должности и структурного подразделения, срок ввода в действие и длительность действия инструкции, подпись, дата, должность, фамилия, имя и отчество лица, утвердившего должностную инструкцию. На последней странице должностной инструкции должна быть предусмотрена подпись лица, принявшего к исполнению настоящую должностную инструкцию.

В разделе 1 «Общие положения» указывается, к какому структурному подразделению относится данная должностная позиция, какое место в этом подразделении она занимает; основное назначение (кем работник является в системе управления и кому непосредственно подчиняется); порядок назначения на должность, перемещения на другие должности (другую работу) и освобождение от данной должности, кто принимает решения по этим вопрос, кем эти решения согласовываются; какими документами и нормативными актами определяется деятельность на данной должности.

В разделе 2 «Квалификационные требования» указываются требуемый уровень профессиональной подготовки (образование) необходимая специализация (специальность), требуемый уровень квалификации (необходимый стаж работы, какая работа или должность должна предшествовать работе на данной должности;

продолжительность; если предварительный стаж работы не требуется, указывается необходимость стажировки или испытательного срока, их продолжительность); уровень знаний (перечень основных дисциплин;

отдельных вопросов, основных нормативно-правовых, технических, технологических, организационных, экономических и других документов, стандартов и т. п.); уровень навыков и умений (что должен работник уметь делать непосредственно сам и вместе с другими в процессе работы на данной должности).

В разделе 3 «Функциональные обязанности» указываются все функциональные обязанности работника на данной должности, выполняемые им непосредственно (самостоятельно) для решения задач, которые должны решаться на данной должности: по вопросам планирования, организации; координации, регулирования, контроля, учета и анализа в отношении основных элементов производственных процессов (сырья и материалов, рабочих, технологического оборудования, машин, механизмов, финансов информации, готовой продукции и т. п.) и условий производства (технологии, техники безопасности, контроля качества и т.п.), а также все функциональные обязанности, которые работник на данной должности выполняет совместно с другими работниками системы управления.

В разделе 4 «Права» перечисляются права, необходимые для выполнения каждой функциональной обязанности. Для сокращения, объёма данного раздела одинаковые права, необходимые для выполнения различных функциональных обязанностей, могут быть сгруппированы.

Раздел 5 «Ответственность» разрабатывается в точном соответствии со структурой и содержанием разделов «Функциональные обязанности» и «Права», т. е. по каждому пункту прав и обязанностей должны быть установлены вид (административная, материальная или уголовная) и мера (степень) ответственности. В этом разделе, как и в разделе «Права», ответственность может быть сгруппирована по отдельным видам: административная, материальная или уголовная.

Однако здесь группировка должна производиться только в том случае, если совпадает мера ответственности.

В следующих разделах учебного пособия будут рассмотрены приемы и методы по организационному проектированию деятельности СБП, используемых для разработки структур основных подразделений и должностных инструкций различных категорий специалистов, работающих в службе безопасности.

Контрольные вопросы

1. Дайте характеристику трех видов управленческой деятельности социальных организационных систем.
2. Назначение организационного проектирования (три задачи).
3. Назовите основные этапы проектирования функциональной управленческой деятельности.
4. В чем состоит суть проектирования организационной структуры системы управления?
5. Какие виды документов разрабатываются при организационном проектировании систем управления?
6. Опишите типовое содержание положения о функциональных структурах подразделения.
7. Что должно быть включено в должностные инструкции работников системы управления?

Глава 4. Структура и функции службы безопасности предприятия

4.1. Состав службы безопасности предприятия

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю фирмы.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя фирмы по безопасности.

Структура, численность и состав службы безопасности фирмы определяются реальными финансовыми возможностями, масштабом коммерческой деятельности, степенью конфиденциальности информации. В зависимости от этих факторов служба безопасности может варьировать от двух-трех человек, работающих по совместительству, до полномасштабной службы с развитой структурой (несколько десятков и сотен человек).

Наиболее полный состав в виде отделов, групп или отдельных специалистов СБП может включать следующий набор организационных структур:

. подразделение охраны;
. подразделение режима;
. подразделение по работе с кадрами;
. подразделение по работе с документами с грифом «Коммерческая тайна» (специальный отдел);
. подразделение инженерно-технической защиты;
. подразделение разведки;
. подразделение контрразведки;
. подразделение информационно-аналитической деятельности;
. подразделение (служба) защиты информации.

Следует отметить, что в реальных условиях функции названных подразделений могут выполняться путем их совмещения, а также одним или несколькими специалистами.

4.2. Основные функции службы безопасности предприятия

На службу безопасности предприятия возлагаются следующие основные функции [13]:

. организация и обеспечение пропускного и внутриобъектового режима в зданиях и помещениях, определение порядка несения службы охраны, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;

. руководство работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

. участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности устава, правил внутреннего трудового распорядка, положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

. разработка и осуществление совместно с другими подразделениями мероприятий по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной;

. изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, а также учет и анализ нарушений режима безопасности;

. организация и проведение служебных расследований по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;

. разработки и учет перечня сведений, составляющих коммерческую тайну и других нормативных актов, регламентирующих порядок обеспечения безопасности и защиты информации;

. обеспечение строгого выполнения требований нормативных документов по защите коммерческой тайны;

. осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений в части оговоренных в договорах условий по защите коммерческой тайны;

. организация и проведение учебы сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к охране коммерческих секретов был глубоко осознанный подход;

. ведение учета сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

. ведение учета выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

. поддержка контактов с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

На основе сформулированных функций и задач может быть рекомендована следующая схема целевой функции (дерево целей) службы безопасности предприятия (рис. 4.1.).

Виды основных функций, которые может выполнить служба безопасности, перечислены в ст. 3 закона РФ «О частной детективной и охранной деятельности в Российской Федерации».

При этом в своей практической деятельности служба безопасности не должна выходить за пределы своих полномочий. Анализ зарубежной и отечественной литературы, текущего законодательства и практика функционирования служб безопасности различных организаций позволяет кратко охарактеризовать наиболее часто выполняемые функции.

Приведенный набор подцелей реализуется в определенных видах деятельности предприятия конкретными видами работ. Наиболее важные из них были описаны и систематизированы В.П. Мак-Маком [7].

Рассмотрим их более подробно на конкретных примерах.

Рис. 4.1. Дерево целей функционирования СБП

4.2.1. Охрана имущества предприятия

Под охраной имущества понимается комплекс оперативно-режимных, организационно-управленческих и инженерно-технических действий, проводимых с целью обеспечения сохранности материально-технических и финансовых средств собственника. Охране подлежат все материальные ценности независимо от их местоположения (внутри или за пределами предприятия).

В то же время существуют объекты первостепенной важности, охране которых необходимо уделять особое внимание, так как именно они чаще всего подвергаются противоправному посягательству. К таким объектам относятся:

• дорогостоящие сырьевые ресурсы (нефть, древесина, золото и т.д.);
• дефицитное оборудование (компьютеры, автозапчасти и т.д.);
• продовольственные и промышленные товары;
• деньги, инвалюта и т.д.;
• наиболее важная и конфиденциальная документация;
• земельные угодья, участки и т.д.

Пятиугольник: Устранение причиненного ущерба

Пятиугольник: Меры по ликвидации угроз и конкретных преступлений

Пятиугольник: Своевременное определение реальных угроз и конкретных преступлений

Пятиугольник: Превентивные меры по обеспечению безопасности

Пятиугольник: Систематический контроль возможности появления реальных или потенциальных угроз безопасности

Подпись: Подцели

Подпись: Ликвидацией последствий

Подпись: Локализацией преступных действий

Подпись: Обнаружением угроз

Подпись: Выявлением угроз

Подпись: Предупреждением угроз

Подпись: Обеспечение безопасности предприятия.

Совершенно очевидно, что охране именно этого имущества должно быть уделено главное внимание.

4.2.2. Организация обеспечения пропускного и внутриобъектового режима в зданиях и помещениях

Задачи:

1. Организация пропускного и внутриобъектного режима.

2. Разработка разрешительной системы и обеспечение допуска сотрудников к документам, материалам и сведениям, составляющим коммерческую тайну.

3. Контроль за соблюдением режима допуска к сведениям и документам.

4. Совершенствование системы пропускного и внутри объектного режима.

5. Участие в разработке "Перечня сведений, составляющих коммерческую тайну".

4.2.3. Расследование факторов разглашения коммерческой тайны предприятия

Под коммерческой тайной понимается не являющаяся государственным секретом, специально охраняемая собственником (владельцем) управленческая, производственная, научно-техническая, финансовая, торговая и иная деловая информация.

Таким образом, любая конфиденциальная информация, представляющая

ценность для предприятия в достижении преимуществ над конкурентами и извлечения

прибыли, может стать коммерческой тайной предприятия. Не вдаваясь в методику определения информации, составляющей коммерческую тайну (она описана в многочисленных публикациях), отметим, что таковой она становится только после утверждения руководством предприятия «Перечня сведений, составляющих коммерческую тайну предприятия» и объявления его под расписку всем причастным к ней сотрудникам.

Следует, однако, при этом учесть, что в соответствии с Постановлением РСФСР от 05.12.91 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну», не могут составлять коммерческую тайну:

• учредительные документы (разрешение о создании предприятия или договор учредителей) и устав;

• документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);

• сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

• документы о платежеспособности;

• сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

• документы об уплате налогов и обязательных платежах;

• сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

• сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

По факту разглашения коммерческой тайны предприятия служба безопасности должна проводить расследование по следующим направлениям: 1) человек; 2) документ; 3) изделие-процесс. Именно в рамках этой триады (разумеется, при ее конкретизации) расположены каналы утечки информации, поэтому наиболее целесообразно организовать работу службы безопасности по перечисленным направлениям.

4.2.4. Сбор информации о лицах, заключивших с предприятием контракты

Предприятие обычно заключает два типа контрактов: коммерческий (документ, представляющий собой договор поставки товаров или предоставления услуг) и трудовой (вид трудового договора, заключающегося в письменной форме со своими постоянными или временными работниками). Одним из договорных условий может быть письменное согласие лица, с кем подписывается контракт, на сбор информации об его биографических и других характеризующих личность данных. При этом в контракте должно быть оговорено, что такого рода сбор информации проводится как до вступления контракта в силу (например, во время прохождения испытательного срока), так и во время его реализации, т.е. до расторжения контракта.

Содержание такой информации о личности проверяемого должно, на наш взгляд, включать следующие сведения:

• преступления и административные проступки, совершенные им в прошлом;

• судебные процессы по гражданским делам, в которых он выступал в качестве истца или ответчика;

• качество исполнения ранее заключаемых договоров с другими партнерами;

• аморальные проступки (пьянство, внебрачные связи, наркотики и т.д.);

• суждения бывших сослуживцев и руководителей о его профессиональных и моральных качествах;

• болезни, которые он перенес ранее;

• материальное положение;

• случаи увольнения с работы по отрицательным мотивам, не нашедшие отражение в трудовой книжке;

• участие в организациях, дискриминирующих по признакам пола, расы, цвета кожи, убеждениям, религиозной и национальной принадлежности;

• жизнь не по средствам;

• наличие значительных финансовых накоплений сомнительного происхождения;

• необоснованный и нелогичный отказ от продвижения по службе, перевода на новое место работы;

• жалобы клиентов и других лиц, контактирующих с проверяемым;

• прогулы и частые отвлечения от выполнения служебных обязанностей;

• задержки по надуманным предлогам на работе после окончания рабочего дня;

• систематические посещения проверяемого лицами, не имеющими отношения к его служебным обязанностям;

• факты отказа от использования очередного отпуска;

• результаты различных тестов;

• семейные проблемы;

• долги и займы и т.д.

Представляется, что совокупность указанных сведений в достаточной мере может характеризовать человека и помочь руководству предприятия принять решение о целесообразности дальнейшего с ним сотрудничества.

4.2.5. Выявление некредитоспособных партнеров

Некредитоспособным признается тот партнер, у которого для получения кредита нет предпосылок, подтверждающих способность возвратить его.

Некредитоспособного партнера характеризуют следующие действия:

• неаккуратность при расчетах по ранее полученным кредитам;

• ухудшение текущего финансового положения;

• неспособность при необходимости мобилизовать денежные средства из различных источников;

• обналичивание денежных средств в объемах, превышающих размеры фонда зарплаты;

• удержание им (без согласия партнера) денежных средств, полученных в качестве кредита или предварительной оплаты;

• совершение операций с банковскими документами, не обеспеченными кредитными ресурсами;

• нецелевое использование кредитных средств или их получение по фиктивным документам;

• попытка оттянуть выплату денежных средств партнеру при добросовестном выполнении им условий контракта и т.д.

Служба безопасности обязана выявлять некредитоспособных партнеров как до заключения, так и в процессе реализации договора и своевременно информировать об этом руководство предприятия.

4.2.6. Выявление ненадежных партнеров

Ненадежность делового партнера определяется:

• большим количеством сорванных по его вине сделок с другими фирмами;

• несвоевременным и некачественным выполнением условий заключенных договоров;

• значительным количеством в фирме ранее судимых лиц;

• фактами ведения против предприятия-учредителя экономического шпионажа;

• использование помощи сотрудников правоохранительных органов, налоговых инспекций и т.д. с целью парализации экономической деятельности своего партнера;

• умышленным затягиванием деловых переговоров;

• неуважительным отношением к авторскому или патентному праву;

• предъявлением к нему значительного количества судебных исков;

• наличием большого долга;

• непрочной позицией на рынке;

• нерегулярной и ненадежной поставкой сырья и товаров;

• отсутствием доверия потребителей;

• испорченной репутацией среди деловых кругов.

Способность службы безопасности своевременно выявить хотя бы отдельные параметры ненадежности будущих или настоящих деловых партнеров в значительной степени может повлиять на степень экономической безопасности предприятия-учредителя.

4.2.7. Установление обстоятельств недобросовестной конкуренции со стороны других предприятий

Под недобросовестной конкуренцией понимается применение в конкурентной борьбе средств и методов, связанных с нарушением действующего законодательства, регламентирующего производственную и коммерческую деятельность предприятий или норм и правил взаимоотношений между конкурентами, принятых на рынке товаров и услуг.

Известны следующие формы недобросовестной конкуренции:

• установление контроля над деятельностью конкурента с целью прекращения этой деятельности;

• установление дискриминационных цен или коммерческих условий;

• ложная реклама;

• установление зависимости поставок конкретных товаров или услуг от принятых ограничений в отношении производства или распределения конкурирующих товаров;

• введение ограничительных условий в агентские соглашения;

• тайный сговор на торгах и создание тайных картелей;

• нарушения качества, стандартов и условий поставок товаров и услуг;

• подделка и производство оригинальных изделий, выпускаемых конкурентом;

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

• злоупотребление господствующим положением на рынке (например, чрезмерное завышение цен или отказ осуществлять поставки);

• установление дискриминационных коммерческих условий;

• распространение ложных, неточных или искаженных сведений, способных причинить убытки хозяйствующему субъекту либо нанести ущерб его деловой репутации;

• введение потребителей в заблуждение относительно характера, способа и места изготовления, потребительских свойств, качества товара;

• некорректное сравнение хозяйствующим субъектом в процессе его рекламной деятельности, производимых или реализуемых им товаров с товарами других хозяйствующих субъектов;

• несанкционированное приобретение и использование фирменных секретов конкурента;

• самовольное использование товарного знака, фирменного наименования или маркировки товаров;

• получение, использование, разглашение научно-технической, производственной или торговой информации, в т.ч. коммерческой тайны, без согласия ее владельца.

Недобросовестная конкуренция возможна путем использования коррумпированных чиновников, лиц из уголовной среды и экономических шпионов.

4.2.8. Расследование фактов неправомерного использования товарных (фирменных) знаков предприятия

Товарный знак – это обозначение, способное отличать соответственно товары и услуги одних юридических и физических лиц от однородных товаров и услуг других юридических или физических лиц.

Нарушением прав владельца товарного знака признается несанкционированное изготовление, применение, ввоз, предложение к продаже, продажа, иное введение в хозяйственный оборот или хранение с этой целью товарного знака или товара, обозначенного этим знаком, или обозначения, сходного с ним до степени смешения в отношении однородных товаров. Важнейшей особенностью такого нарушения является его большой территориальный разброс, наличие большого количества потенциальных правонарушителей и сложности с его документированием, что чрезвычайно затрудняет деятельность сотрудников службы безопасности.

4.2.9. Изучение негативных аспектов рынка

Под рынком понимается сфера товарного обращения, товарооборота, выявляющая и устанавливающая общественно необходимые затраты труда на производство товара. Комплексный анализ рынка проводит специально предназначенная для этого служба предприятия, которая, наряду с официальной экономической информацией, использует сведения, представленные службой безопасности. Такие сведения могут быть сведены в два блока: 1) состояние и влияние теневой экономики на рынок и 2) криминальные аспекты рынка.

Теневая экономика (т.е. вся экономическая деятельность, которая по каким-либо причинам не учитывается официальной статистикой и не включается в валовый национальный продукт) состоит из двух частей:

1) экономическая деятельность, являющаяся вполне легальной, нескрываемой деятельностью, но не подвергающаяся налогообложению и по разным причинам не учитываемая официальной статистикой;

2) противозаконная, преднамеренно скрываемая экономическая деятельность.

Изучение криминальных аспектов рынка, обычно, включает в себя:

• криминологическую зараженность существующих или потенциальных потребителей (клиентов);

• криминологическую обстановку на территории функционирования рынка и тенденции его развития;

• реакцию сотрудников правоохранительных органов на совершаемые правонарушения, затрагивающие интересы предприятия;

• состояние правонарушений в сфере кредитно-финансовой системы;

• криминологические последствия введения приватизации;

• характеристику правонарушений, совершаемых в отношении товаров и услуг, производимых (предлагаемых) предприятием-учредителем, степень текущего и потенциального материального ущерба предприятию от правонарушений на рынке и т.д.

4.2.10. Сбор информации для проведения деловых переговоров

Основными стадиями переговоров являются:

1) подготовка к переговорам;

2) процесс их ведения;

3) анализ результатов переговоров и выполнение достигнутых договоренностей.

Сотрудники службы безопасности участвуют в сборе информации на первой и второй стадиях. При всей условности такого деления служба безопасности должна представлять на различных стадиях руководству предприятия-учредителя свою информацию, например в процессе подготовки к переговорам сведения об участниках будущих переговоров, их сильных и слабых сторонах, их позициях и планах ведения переговоров, подготовленных материалах, конкурентоспособности и платежеспособности делового партнера и т.д.

Во время проведения переговоров служба безопасности должна поставлять информацию об изменениях позиции партнеров по переговорам, о возможных попытках с их стороны шантажировать, подкупать членов делегации предприятия-учредителя, а также о проведении разведывательных мероприятий в отношении их и т.д.

4.2.11. Обеспечение порядка в местах проведения предприятием представительских, конфиденциальных и массовых мероприятий

Обеспечение порядка необходимо во время проведения мероприятий:

• представительских (выставки, ярмарки и т.д.);

• массовых (спортивные соревнования, концерты и т.д.);

• конфиденциальных (заседание правления, совещания руководителей и специалистов по служебным вопросам и т.д.).

В зависимости от их типа меняется и содержание деятельности службы безопасности. Так, при проведении закрытых совещаний основное внимание уделяется, прежде всего, защите сведений, составляющих коммерческую тайну, на выставках необходимо принимать меры к недопущению кражи или порчи имущества предприятия; при проведении концертов основное внимание уделяется физической безопасности людей и т.д.

4.2.12. Консультирование и представление рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности

В обязанности службы безопасности входит не только консультирование и дача рекомендаций сотрудникам предприятия по вопросам обеспечения безопасности, но и ее реализация. В связи с этим необходимо внести в проект устава службы безопасности положение об обязанности сотрудников подразделений предприятия выполнять эти рекомендации и определить ответственность (материальную и дисциплинарную) за их невыполнение. Проведение консультаций и рекомендаций по вопросам безопасности обычно не выходит за пределы таких ее основных видов, как экономическая, информационная, пожарная, физическая безопасность.

4.2.13. Проектирование, монтаж и эксплуатационное обслуживание средства охранно-пожарной сигнализации

Средства охранно-пожарной сигнализации предназначены для обнаружения попыток проникновения на объект и возникновения пожара, оповещения сотрудников службы безопасности о появлении и нарастании этих угроз и обеспечения контроля доступа на охраняемый объект. Деятельность подразделения службы безопасности, осуществляющего функцию внедрения и эксплуатации охранно-пожарной сигнализации, осуществляется в несколько этапов. Первый этап (проектирование) предусматривает планирование работ по внедрению и капитальному ремонту средств сигнализации, обследование объекта с целью получения исходных данных для разработки исполнительной проектно-сметной документации; материально-техническое обеспечение монтажных работ. На этапе выполнения монтажных работ, для проведения которых обычно приглашаются специализированные организации, осуществляется технический надзор за качеством их производства, особенно при проведении пусконаладочной работы.

Наконец, последний этап (эксплуатационное обслуживание) включает в себя:

• сдачу этих средств в эксплуатацию;

• планирование эксплуатационных мероприятий и контроль за их исполнением;

• техническое обслуживание, технический контроль за эксплуатацией средств сигнализации;

• ремонт приборов и аппаратуры охранно-пожарной сигнализации;

• материальное обеспечение эксплуатационных нужд;

• ведение установленной технической документации;

• сбор и обобщение статистических данных по эксплуатационно-техническому обслуживанию;

• анализ причин отказов в работе аппаратуры и причин, способствующих совершению краж и пожаров с заблокированных участков объекта.

4.2.14. Защита жизни и здоровья персонала от противоправных посягательств

Защиту организует служба безопасности либо всего персонала предприятия (во время нахождения его на работе), либо некоторых его категорий (руководители, кассиры и т.д.) в рабочее и, как исключение, в нерабочее время, либо применяются оба варианта. При этом четко определяется время (круглосуточно, только в дневное время и т.д.) проведения охранных мероприятий. Охранники должны быть нацелены прежде всего на пресечение насильственных преступлений (покушение на убийство, рэкет) и административных проступков (мелкое хулиганство) в отношении охраняемых лиц. Должны широко применяться технические средства защиты.

4.2.15. Поиск утраченного имущества предприятия

Под имуществом предприятия понимается находящиеся в его ведении или собственности материальные ценности, денежные средства в кассе, на расчетном счете и других счетах в банках, нематериальные активы (патенты, лицензии, программы, ноу-хау, брокерские места и т.п.). В узком смысле слова под имуществом предприятия понимаются вещи (материальные ценности).

Утраченное имущество предприятия условно делится на две категории:

• ставшее бесхозяйным (т.е. собственник которого неизвестен);

• утерянное по халатности его сотрудников.

Первую категорию характеризуют следующие признаки:

1) имущество утеряно при неизвестных обстоятельствах;

2) информация о пропаже поступает, как правило, с опозданием;

3) закрепление за утерянным имуществом либо не произведено, либо сделано формально;

4) само имущество, за редким исключением, является громоздким или большим (грузовые автомашины, экскаваторы, трубы и т.д.);

5) охрана имущества не выставляется, а при ее наличии передача охраняемого имущества по смене не производится.

Признаки, характеризующие утерянное имущество по халатности сотрудников, следующие:

1) его относительно малые габариты или ценные бумаги (калькуляторы, деньги, документы и т.д.);

2) очевидность вины конкретного сотрудника;

3) известны место и время (иногда приблизительно) пропажи;

4) неизвестны способы пропажи имущества. Объединяет их одно: нанесение материального (иногда значительного) ущерба предприятию. Содержание работы сотрудников службы безопасности в зависимости от категории утраченного имущества носит различный характер.

4.2.16. Сбор сведений по гражданским делам

Известно, что в рамках гражданского производства судами рассматриваются споры о праве гражданском, затрагивающем права и законные интересы юридического лица (в нашем случае, предприятия); в предусмотренных законом случаях дел по жалобе на

действия административных органов или должностных лиц, совершенные с нарушением их полномочий; дела об установлении фактов, имеющих юридическое значение, рассматриваемые и разрешаемые судом.

Сбор сведений по гражданским делам служба безопасности осуществляет во взаимодействии с представителем предприятия-учредителя на суде как до, так и во время рассмотрения их на судебных заседаниях. Необходимость в сборе информации сотрудниками службы безопасности возникает обычно в случаях:

• выявления свидетелей и документов;

• проверки достоверности информации участников процесса и подлинности доказательств, представленных на суде;

• возникновения необходимости проверки наличия основания для отвода в рассмотрении дела;

• оказания помощи суду в установлении фактического местонахождения участников процесса;

• выявления лиц, оскорбляющих или оклеветавших руководителей предприятия-учредителя;

• поиска утаиваемого от суда имущества процессуального противника, необходимого для погашения материального ущерба;

• необходимости выявления среди свидетелей лиц, которые в силу своих физических или психических недостатков не способны правильно воспринимать факты или давать о них правильные показания и т.д.

4.2.17. Розыск без вести пропавших сотрудников

Без вести пропавшим считается лицо, исчезнувшее внезапно, без видимых к тому причин, местонахождение и судьба которого остается неизвестной.

Все случаи безвестного исчезновения сотрудников можно разделить на четыре группы:

• связанные с криминальным характером происшедшего (убийство, наезд транспорта со смертельным исходом и т.д.);

• обусловленные некриминальным лишением жизни пропавшего (самоубийство, утопление и т.д.);

• объективно не зависящие от сознания и воли сотрудников и не носящие криминальный характер (уход из дома вследствие психического заболевания, административный арест и т.д.);

• вызванные проблемами личного и служебного характера (семейные неурядицы, ссора с начальством и т.д.).

Сотрудники службы безопасности подключаются к розыску без вести пропавшего сотрудника только в том случае, если есть основания предполагать, что его отсутствие на работе приведет (может привести) к реальному или потенциальному ущербу предприятию. Деятельность службы безопасности по розыску без вести пропавшего сотрудника – это комплекс мероприятий, осуществляемых при тесном взаимодействии с органами внутренних дел с целью установления фактических обстоятельств его исчезновения и фактического местонахождения.

Рассмотренные реальные ситуации, связанные с деятельностью СБП, могут быть рекомендованы для проведения практических работ и организации деловых игр или при обучении студентов и специалистов по вопросам организационной защиты информации.

4.3. Построение структурной схемы управления службой безопасности предприятия

Структура, численность и состав СБП определяются реальными потребностями предприятия и степенью конфиденциальности ее информации. В зависимости от масштабов организации ее безопасность и защита информации могут быть обеспечены по-разному: от абонементного обслуживания силами частных охранных и детективных

структур до развертывания полномасштабной собственной службы и системы безопасности с развитой структурой и штатной численностью.

Опорными точками такой структуры являются (рис. 4.2.):

1. Ответственный руководитель системы.

2. Совет по безопасности предприятия.

3. Служба безопасности предприятия в составе отделов: охраны, режима, кадров, документов с коммерческой тайной, инженерно-технических средств безопасности и контрразведывательной и информационно-аналитической деятельности и защиты информации;

4. Линейные подразделения предприятия, активно участвующие в обеспечении экономической безопасности (кадровое, финансовое, плановое, юридическое, маркетинга и др.).

Рис. 4.2. Схема управления СБП

Решение о создании системы безопасности принимается руководством предприятия в соответствии с ее уставом (прил. 1).

Ответственный руководитель системы безопасности предприятия – это либо сам директор, либо один из его заместителей. Он должен хорошо знать, что подлежит защите и охране и обладать определенными познаниями в области безопасности.

Совет по безопасности предприятия – это коллегиальный орган при руководителе системы безопасности. Совет выполняет

Подпись: Подразделения СБП

Подпись: Кризисная группа

Подпись: Группа оперативного реагирования

Подпись: Начальник службы безопасности

Подпись: Юрисконсульт по безопасности

Подпись: Совет по безопасности

Подпись: Ответственный руководитель предприятия консультативные функции, а его предложения носят рекомендательный характер. Все члены совета назначаются директором из числа ведущих специалистов, имеющих опыт работы или заинтересованных в обеспечении безопасности.

Основными задачами совета являются [13]:

. оценка и выработка основных направлений деятельности фирмы по обеспечению экономической безопасности;

. разработка перспективных программ совершенствования системы безопасности;

. разработка предложений о содержании и характере взаимодействия с правоохранительными органами, органами местного управления, с соседними СБФ, а также с партнерами, заказчиками, потребителями продукции с целью соблюдения конфиденциальности, установления и поддержания других мер безопасности;

. организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;

. организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;

. предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;

. выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;

. обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, связанные с деловым сотрудничеством как на национальном, так и на международном уровне;

. обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;

. обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;

. оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

В своей деятельности служба безопасности руководствуется инструкциями:

• по организации режима и охраны;

• защите коммерческой тайны;

• работе с конфиденциальной информацией для руководителей, специалистов и технического персонала;

• организации хранения дел, содержащих конфиденциальную информацию, в архиве;

• инженерно-технической защите информации;

• о порядке работы с иностранными представителями и представительствами, а также перечнем сведений, составляющих коммерческую тайну.

С целью более широкого охвата и качественного исполнения требований защиты коммерческой тайны решением руководства предприятия и службы безопасности могут создаваться отдельные комиссии, выполняющие определенные контрольно-ревизионные функции на временной или постоянной основе, в том числе:

. квартальные или годовые комиссии по проверке наличия, состояния и учета документов (материалов, сведений, ценностей);

. комиссия по оценке возможностей публикации периодических документов, объявлений, проспектов, интервью и других выступлений в печати, на радио и телевидении, семинарах, симпозиумах, конференциях и т.п.;

. периодические проверочные комиссии для проверки знаний и умения выполнять требования нормативных документов по защите коммерческой тайны, а также для оценки эффективности и надежности защитных мероприятий по обеспечению безопасности предприятия.

Контрольные вопросы

1. Какие подразделения входят в состав СБП?
2. Назовите основные функции СБП.
3. Каким законом регламентируются функции СБП?
4. По каким направлениям производится расследование факта разглашения коммерческой тайны?
5. Чем определяется состав СБП?
6. Перечислите задачи, выполняемые советом по безопасности предприятия.

Глава 5. Подразделения службы безопасности предприятия

5.1. Подразделения режима и охраны
5.2. Специальный отдел
5.3. Подразделения информационно-аналитической деятельности
5.4. Подразделения инженерно-технической защиты
5.5. Подразделения разведки

5.1. Подразделения режима и охраны

Две функции службы безопасности предприятия – обеспечение режима и охраны – являются близкими по их кадровому и техническому обеспечению и на многих предприятиях реализуются в виде одного отдела по режиму и охране. В состав отдела в этом случае входят сектор режима и сектор охраны, который, в свою очередь, может включать комендантскую службу и группу личной охраны руководства.

Основными задачами организации режима и охраны являются:

. предупреждение проникновения в служебные помещения, в охраняемые зоны и на территорию объекта посторонних лиц;

. обеспечение порядка вноса (выноса), ввоза (вывоза) материальных ценностей и входа (выхода) сотрудников и клиентов.

Все помещения предприятия в зависимости от назначения и характера совершаемых в них актов, действий или операций разделяются на несколько зон доступности (безопасности), которые учитывают степень важности различных частей объекта с точки зрения возможного ущерба от криминальных угроз. Зоны безопасности располагаются последовательно, от забора на территории объекта до хранилища ценностей и информации, создавая цепь чередующихся препятствий, которые придется преодолевать злоумышленнику.

Внутриобъектовый режим

Внутриобъектовый режим – это установленный в фирме порядок выполнения правил внутреннего трудового распорядка, направленных на обеспечение экономической безопасности, сохранение материальных средств и защиту конфиденциальной информации [13].

Внутриобъектовый режим предусматривает следующие основные требования:

• установление четкого распорядка рабочего времени;

• строгое соблюдение сотрудниками правил экономической и информационной безопасности, правил противопожарной и противоаварийной безопасности и техники безопасности;

• установление порядка приема и работы с посетителями сторонних организаций;

• оборудование фирмы техническими средствами обеспечения производственной деятельности (связь, автоматизация, охранная и пожарная сигнализация, замки, ограждения и др.);

• порядок сдачи и приема помещений под охрану;

• порядок ведения телефонных, факсовых и телекоммуникационных обменов информацией с соблюдением режима конфиденциальности и экономии.

Особое внимание в построении внутриобъектового режима отводится работе с представителями сторонних организаций, которая осуществляется в следующем порядке [13]:

. принимающий специалист накануне делает заявку канцелярии на следующий день с указанием Ф.И.О. прибывающих, их места работы и времени предполагаемого прибытия;

. в день прибытия приглашенных канцелярия фиксирует их прибытие в журнале учета посетителей и приглашает специалиста фирмы;

. специалист встречает прибывших, получает в канцелярии ключи от комнаты переговоров и сопровождает туда посетителей.

Запрещается прием представителей сторонних организаций в других помещениях офиса без специального на то разрешения директора или его заместителя;

. в ходе работы необходимо плотно закрывать окна и шторы;

. по окончании работы с посетителями принимающий их специалист провожает их до выхода из офиса и делает в журнале учета посетителей соответствующие заметки о времени их ухода. Во время пребывания посетителей принимающий специалист обязан контролировать их пребывание и действия. После завершения встречи специалист фирмы закрывает комнату переговоров и сдает ключи от нее канцелярии.

Не менее важным в разработке комплекса мероприятий внутриобъектового режима является пропускной режим.

Пропускной режим – это установленный в фирме, организации,

на предприятии порядок, при котором исключается возможность бесконтрольного прохода (проезда), вноса (выноса) материальных ценностей.

Проход (проезд) сотрудников, служащих и других лиц на территорию охраняемого объекта и обратно, внос и вынос материальных ценностей производится по пропускам через контрольно-проходные и проездные переходы.

Пропускной режим предусматривает:

. установление определенного порядка допуска на территорию объекта рабочих и служащих данного объекта и посетителей;

. установление определенного порядка вывоза (выноса), ввоза (вноса) продукции и материальных ценностей;

. устройство ограждения, освещения, оборудование контрольно-проходных и проездных пунктов (постов) и бюро пропусков средствами сигнализации, связи и др. необходимой техникой, обеспечивающей осуществление пропускного режима, а также обеспечение их документацией и инвентарем;

. определение круга должностных лиц, имеющих право выдачи и подписи всех видов пропусков;

. оборудование камер хранения личных вещей и площадок для личного автотранспорта.

Охранная деятельность

Основные направления охранной деятельности СБ показаны на рис. 5.1.

Рис. 5.1. Основные направления охранной деятельности [13]

Каждое из указанных направлений имеет свои особенности при обеспечении безопасности конкретного объекта защиты.

Объектами охраны выступают:

• стационарные объекты;
• подвижные объекты;
• персонал;
• денежные средства, ценные бумаги и другие ценности.

Таким образом, эффективность системы защиты оценивается как время с момента возникновения угрозы до начала ее ликвидации. Чем сложнее и разветвленнее система защиты, тем больше времени требуется на ее преодоление и тем больше вероятность того, что угроза будет обнаружена, определена, отражена и ликвидирована.

Режим охраны объекта по времени может иметь круглосуточный, частичный (определенные часы суток) или выборочный характер. В зависимости от количества используемых сил и средств, плотности

Выноска со стрелкой влево:

? Обеспечение взаимодействия с органами внутренних дел, судами и таможнями и др.

Выноска со стрелкой влево: Объекты охраны:

? Стационарные

? Подвижные

? Транспортные перевозки

Выноска со стрелкой влево: Объекты:

? Руководящий состав фирмы и члены их семей

? Ведущие специалисты фирмы

Подпись: Обеспечение порядка в местах массовых мероприятий

Подпись: Консультирова-ние и подготовка рекомендации по вопросам правомерной защиты от противоправных посягательств

Подпись: Проектирование, монтаж и эксплуатационное обслуживание средств охранно-пожарной сигнализации

Подпись: Охрана имущества собственников, в том числе и при транспорти-ровке

Выноска со стрелкой влево: Объекты:

? Здания и помещения

? Технические средства обеспечения производствен-ной и трудовой деятельности

Подпись: Защита жизни и здоровья людей

Выноска со стрелкой влево:

? Конструирование сотрудников фирмы по вопросам экономической безопасности

? Обучение сотрудников охраны

Подпись: Виды охранной деятельностиконтроля территории и объекта режим охраны может быть простой или усиленный.

На значительной части охраняемых объектов охранники присутствуют круглосуточно. В дневное время они контролируют посетителей, прибывающих на объект, осуществляют контрольно-пропускной режим, а в ночное время несут закрытую охрану объекта, принимая на себя полную ответственность за его сохранность.

Некоторые объекты охраняются лишь эпизодически, т.е. выборочно по времени.

Существует несколько видов охраны, в том числе [13]:

• охрана с помощью технических средств – с подключением на пульт централизованного наблюдения и с установкой автоматической сигнализации;

• охрана путем выставления постов (силами отдела охраны или милиции);

• комбинированная охрана.

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

Основными принципами организации режима охраны являются:

. активность и предупредительный характер охраны,заключающиеся в опережающем выявлении признаков готовящейся атаки объекта и своевременном принятии мер по ее предупреждению или пресечению (отражению);

. целесообразность и обоснованность организации режима охраны объекта, своевременность его усиления, рациональное использование сил и средств охраны;

. разумное сочетание собственных возможностей и возможностей сил правоохранительных органов для обеспечения безопасности объекта;

. осуществление охраны по единому плану;

. скрытность или демонстративность охраны в зависимости от ситуации, складывающейся вокруг охраняемого объекта;

. максимальная информированность охраны обо всех событиях, происходящих на объекте, условиях коммерческих сделок фирмы и т.п. для правильного определения ключевого звена, воздействие на которое позволяет обеспечить безопасность объекта.

В практике деятельности подразделений охраны по обеспечению безопасности объекта выделяются две группы задач [13]:

• аналитические и предупредительные задачи;

• процедурно-отражательные задачи.

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

Решение предупредительных задач связано в первую очередь с созданием имиджа сильного и надежного режима охраны. Подобный имидж может быть создан серией имитационных мероприятий, демонстрирующих "неудачные" попытки посягательства на объект и мощное противодействие охраны преступникам. Все это может быть дополнено впечатляющей демонстрацией элементов режима охраны (внушительного вида охранники, современная охранная сигнализация, присутствие милиции на объекте и т. д.). Предупредить покушение на охраняемый объект можно также путем его маскировки, перекрытия информационных каналов о его деятельности и дезинформацией конкурентов и криминальных элементов о характере деятельности, форме собственности, состоянии режима охраны, объеме имеющихся на объекте товарно-материальных ценностей и т.д.

Вторая группа процедурно-отражательных задач решается путем своевременного обнаружения признаков готовящегося посягательства с последующим его отражением предварительно подготовленными силами и средствами. Как правило, подобное мероприятие (операцию) следует проводить во взаимодействии с сотрудниками органов внутренних дел, которые будут иметь возможность своевременно зафиксировать следы преступной деятельности. В тех случаях, когда время начала посягательства трудно предугадать, имеет смысл в отдельных случаях "подтолкнуть" преступников к началу посягательства. Это может быть достигнуто путем дезинформирования криминальных элементов о времени и месте завоза ценных грузов, крупной суммы денег и т.п.

При организации охраны объекта служба безопасности должна предусмотреть в перечне служебных обязанностей охранников варианты их действий на случай возникновения на объекте или поблизости от него различного рода критических ситуаций. В таких случаях обязанностью охранника является [13]:

. принятие мер к задержанию преступника и сопровождение задержанного в органы внутренних дел;

. обеспечение охраны места происшествия, находящихся на нем следов и вещественных доказательств до прибытия сотрудников милиции;

. оказание помощи пострадавшим от преступления или несчастного случая до прибытия медицинских работников;

. установление свидетелей и очевидцев происшествия, в том числе и для того, чтобы обеспечить самому себе оправдательную свидетельскую базу;

. сообщение в орган внутренних дел о фактах нарушения общественного порядка поблизости от объекта.

Важным условием эффективности охраны стационарных объектов является их техническая укрепленность, наличие на них технических средств обеспечения безопасности.

Элементами технической укрепленности стационарных объектов являются:

• инженерно-технические средства защиты периметра объекта, включающие запретную зону, средства и системы контроля проникновения в нее, контрольно-следовые полосы и другие системы;

• освещение объектов охраны;

• контрольно-пропускные пункты;

• средства видеонаблюдения;

• средства связи.

Основную роль в обеспечении режима охраны выполняют охранники. Задачи и деятельность охраны подчинены прежде всего одной цели – выполнению охранных функций. Охранники при этом должны уметь абстрактно мыслить, импровизировать, быть инициативными, иметь вероятностный подход к событиям, т.е. охранник должен развивать в себе целый ряд качеств – интеллект, здравомыслие, гибкость мышления, физическую силу, чутье, сдержанность и др.

Эти качества должны проявиться при любых формах его деятельности [13]:

• при внутреннем и наружном патрулировании;

• контроле за проходом и проездом персонала;

• в процессе наблюдения;

• проведении расследования;

• наблюдении за деятельностью персонала и посетителей;

• подготовке докладов, справок и других документов;

• преследовании и задержании преступников и нарушителей;

• сопровождении людей и грузов и др.

Охранникам запрещается:

. скрывать от правоохранительных органов ставшие им известными факты готовящихся или совершенных преступлений;

. выдавать себя за сотрудников правоохранительных органов;

. собирать сведения, связанные с личной жизнью, с политическими и религиозными убеждениями отдельных лиц;

. осуществлять видео- и аудиозаписи, фото- и киносъемки в служебных помещениях без письменного согласия на то соответствующих должностных лиц;

. прибегать к действиям, посягающим на права и свободу граждан;

. совершать действия, ставившие под угрозу жизнь, здоровье, честь, достоинство и имущество граждан;

. передавать свою лицензию для использования другими лицами.

5.2. Специальный отдел

Специальный отдел независимо от численности работающих (от одного и более сотрудников) является самостоятельным структурным подразделением и подчиняется непосредственно начальнику СБП.

В наиболее крупных предприятиях этот отдел состоит из следующих структурных единиц:

• сектора обработки секретных документов;

• сектора обработки документов с грифом «Коммерческая тайна»;

• машинописного бюро.

Основной функцией отдела является выполнение и организация работ, связанных с использованием конфиденциальной информации.

Источниками конфиденциальной информации на каждом предприятии являются:

1. Персонал, люди.

2. Документы.

3. Публикации.

4. Технические носители информации.

5. Технические средства обеспечения производственной и трудовой деятельности.

6. Продукция.

7. Промышленные и производственные отходы.

Служба безопасности должна четко знать, у кого (у какого источника) и где (в каком подразделении и в каком виде) присутствует конфиденциальная информация, а также кто способствует неправомерному овладению охраняемыми сведениями.

На рис. 5.2. показаны основные виды конфиденциальной информации, используемой в процессе деятельности предприятия.

Основными функциями отдела являются следующие:

1. Обработка поступающей и отправляемой корреспонденции, доставка ее по назначению.

2. Осуществление контроля за сроками исполнения документов.

3. Организация работы по регистрации, учету и хранению документальных материалов текущего пользования.

4. Разработка номенклатуры дел, контроль за правильным формированием дел в подразделениях и подготовкой материалов к своевременной сдаче в архив.

5. Разработка и внедрение предложений по совершенствованию системы делопроизводства.

6. Печатание и размножение секретных документов и документов с грифом «Коммерческая тайна».

Рис. 5.2. Виды конфиденциальной информации

Подпись: Виды конфиденциальной информации

Подпись: КОММЕРЧЕСКАЯ

Подпись: Сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них

Подпись: ПРОФЕССИОНАЛЬНАЯ

Подпись: Служебные, связанные с коммерческой деятельностью, доступ к которым ограничен законами (коммерческая тайна)

Подпись: Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке

Подпись: Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.)

Подпись: ЛИЧНАЯ

Подпись: Служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна)

Подпись: Сведения, составляющие тайну следствия и судопроизводства

Подпись: Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленном порядке.

Подпись: ПРОИЗВОДСТВЕННАЯ

Подпись: СЛУЖЕБНАЯ

Подпись: СУДЕБНО-СЛЕДСТВЕННАЯ

7. Участие в подготовке созываемых и проводимых руководством закрытых совещаний и организация их технического обслуживания.

8. Специальный отдел по обработке секретных документов руководствуется соответствующими документами по ведению делопроизводства с грифом «Коммерческая тайна», выполняет требования «Инструкции по защите коммерческой тайны».

5.3. Подразделение информационно-аналитической деятельности

Для информационно-аналитической деятельности на более крупных и средних предприятиях создается аналитический центр или специальное подразделение. Основными задачами такого подразделения являются [13]:

. сбор и оперативное использование информации по гражданскому, уголовному и хозяйственному законодательству;

. подготовка и анализ заключаемых договоров, а также подготовка рекомендаций по вопросам правовой защиты от противоправных действий;

. сбор, накопление, обработка, анализ и выдача информации о возможных клиентах и партнерах, перспективах сотрудничества;

. работа с вкладчиками, акционерами, финансовыми брокерами и дилерами с использованием методов экономической разведки;

. подготовка и проведение рекламных кампаний;

. разработка мероприятий по участию фирмы в процессах политического лоббирования, схем поведения по отношению к политическим партиям и общественным движениям;

. сбор и анализ коммерческой информации, в явном или неявном виде присутствующей в средствах массовой информации;

. анализ процессов и тенденций в инвестиционно-финансовой сфере в России и за рубежом;

. сбор информации по конкурирующим фирмам, а также составление психологических портретов их лидеров;

. разработка концепции стратегического развития организации, подготовка, экспертиза и реализация отдельных организационно-финансовых проектов и технологий;

. сбор информации о процессах, происходящих в криминальных структурах, о криминогенной обстановке в районе деятельности фирмы;

. выработка рекомендаций и мер противодействия преступным посягательствам, направленным против банка (фирмы) и их сотрудников.

В аналитическом центре фирмы обычно задействовано несколько сотрудников. Их функции подразделяются на две категории:

• сборщиков информации, занятых добыванием информации из различных источников;

• информационно-аналитических сотрудников.

Ключевая роль в деятельности службы безопасности фирмы должна отводиться аналитическому звену, осуществляющему сбор и обработку информации о конкурентных фирмах и компаниях на товарном рынке, о маркетинговых условиях, криминально-конкурентных действиях.

Таким аналитическим звеном может быть группа информационно-аналитической деятельности.

Цели и задачи такой группы можно сформулировать следующим образом [13]:

• выявление фактических возможностей разглашения, утечки и реализации способов несанкционированного доступа к конфиденциальной информации;

• прогноз вероятных устремлений конкурентов к конкретным материалам и разработкам фирмы;

• выявление причин и обстоятельств, способствующих неправомерному овладению коммерческой информацией;

• оценка надежности и степени защищенности фирмы от внутренних и внешних угроз;

• участие в анализе, разработке и внедрении комплексных экономически и научно обоснованных мер по защите интересов фирмы.

5.4. Подразделение инженерно-технической защиты

К основным средствам инженерно-технической защиты информации относятся следующие:

• физические;

• аппаратные;

• программные;

• математические (криптографические).

Указанные средства применяются для решения следующих задач:

• охраны:

• территории и наблюдения за ней;

• зданий, внутренних помещений и наблюдения за ними;

• оборудования, хранилищ и перемещаемых носителей информации;

. осуществления контролируемого доступа в защищаемые зоны, охраняемые помещения и хранилища;

. создания препятствия визуальному наблюдению, подслушиванию и фотографированию;

. нейтрализации побочных электромагнитных излучений и наводок;

. исключения возможности перехвата электромагнитных излучений средств связи, обработки информации и электронно-вычислительной техники.

Для выполнения этих задач отдел инженерно-технической безопасности осуществляет организационные, организационно-технические и технические мероприятия, наиболее важными из которых являются следующие [7]:

1. Обследование выделенных помещений с целью установления потенциально возможных каналов утечки конфиденциальной информации через технические средства, конструкции зданий и оборудования.

2. Выявление и оценка степени опасности технических каналов утечки информации.

3. Разработка мероприятий по ликвидации (локализации) установленных каналов утечки информации организационными, организационно-техническими или техническими мерами при использовании для этого физических, аппаратных и программных средств и математических методов защиты.

4. Организация контроля (в том числе и инструментального) за эффективностью принятых защитных мероприятий. Проведение обобщения и анализа результатов контроля и разработка предложений по повышению надежности и эффективности мер защиты.

5. Обеспечение приобретения, установки, эксплуатации состояния технических средств защиты информации.

Организационные мероприятия предусматривают:

• определение границ охраняемой зоны (территории);

. технических средств, используемых для обработки конфиденциальной информации в пределах охраняемой зоны (территории);

. опасных с точки зрения возможности образования каналов утечки информации или способов несанкционированного доступа к ней через технические средства;

• реализацию мер локализации или воспрещения возможных каналов утечки конфиденциальной информации или способов НСД к ней;

• организацию контроля (поиска и обнаружения) возможного неконтролируемого излучения опасных сигналов за счет побочных электромагнитных излучений и наводок (ПЭМИН) или специально используемых для этого сигналов;

• организацию строгого контроля прохода и проноса каких-либо предметов, устройств, средств, механизмов в контролируемую зону, способных представлять собой технические средства получения и передачи конфиденциальной информации.

Организационно-технические мероприятия обеспечивают блокирование возможных каналов утечки информации через технические средства обеспечения производственной и трудовой деятельности с помощью специальных технических средств, устанавливаемых на элементы конструкции зданий, помещений и технических средств, потенциально образующих возможные каналы утечки информации.

Для этих целей возможно использование:

• технических средств пассивной защиты: фильтры, ограничители и т.п. средства развязки электрических и электромагнитных сигналов, системы защиты сетей электроснабжения, радио- и часофикации и др.;

• технических средств активной защиты: датчики акустических шумов и электромагнитных помех.

Технические мероприятия обеспечивают приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений и наводок, технических средств обработки конфиденциальной информации или средств, ПЭМИН которых не превышают норм на границе охраняемой территории.

Мероприятия по блокированию несанкционированного получения конфиденциальной информации с помощью технических средств сводятся к следующим основным направлениям, а именно к защите:

• от наблюдения и фотографирования;

• подслушивания;

• перехвата.

Защита от наблюдения и фотографирования предполагает:

. выбор оптимального расположения средств документирования, размножения и отображения (экраны ПЭВМ) информации с целью исключения прямого или дистанционного наблюдения (фотографирования);

. использование светонепроницаемых стекол, занавесок, драпировок, пленок и других защитных материалов и конструкций (решетки, ставни, жалюзи и др.);

. выбор помещений, обращенных окнами в безопасные зоны, направления;

. использование программных средств гашения экранов ПЭВМ после определенного времени работы (работа по режиму времени).

Защита от подслушивания реализуется:

. применением звукопоглощающих облицовок, специальных тамбуров дверных проемов, двойных оконных переплетов;

. использованием средств акустического зашумления объемов и поверхностей (стены, окна, радиаторы отопления, вентиляционные каналы);

. закрытием вентиляционных каналов, систем ввода в помещения отопления, питания, телефонных и радиокоммуникаций, систем охранно-пожарной сигнализации;

. использованием специальных аттестованных помещений, исключающих появление каналов утечки конфиденциальной информации.

Защита от перехвата побочных электромагнитных излучений и наводок самого различного характера обеспечивается:

. размещением источников ПЭМИН на максимально возможном удалении от границы охраняемой (контролируемой) зоны;

. экранированием помещений, средств канальных коммуникаций;

. использованием пространственного и линейного электромагнитного зашумления;

. использованием автономных телефонных систем, локальных систем ЭВМ, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и т.п.);

. развязкой по цепям питания и заземления, размещенным в границах охраняемой зоны;

. использованием подавляющих фильтров в информационных цепях, цепях питания и заземления.

Аттестация защищаемых техническими мерами помещений имеет целью установить наличие в этих помещениях технических средств обеспечения производственной и трудовой деятельности и определить соответствие их характеристик требованиям безопасности.

На каждое такое помещение составляется технический паспорт, в котором указываются технические средства, их типы, номера, реальные технические характеристики и соединительные линии связи, питания, заземления и их состояние.

Технические паспорта помещений хранятся в группе инженерно-технической защиты. При установке или изъятии каких-либо технических средств обязательно внесение изменений в паспорт помещения.

Состав технических средств каждого помещения исследуется на наличие побочных электромагнитных излучений и наводки (ПЭМИН) группой инженерно-технической защиты самостоятельно или с привлечением специализированных организаций, имеющих на это лицензию, необходимую контрольно-измерительную аппаратуру и определенные методики проведения специальных исследований.

С учетом результатов анализа состава технических средств в защищаемых помещениях и результатов их специсследований устанавливается опасность тех или иных устройств как потенциальных источников образования каналов утечки охраняемых сведений, и вырабатываются целесообразные мероприятия по их локализации.

5.5. Подразделение разведки

В условиях обострения конкурентной борьбы и роста преступности роль и значение разведки службы безопасности предприятия будет постоянно повышаться. Перед подразделением обычно ставится одна общая цель: своевременное выявление и предоставление руководству предприятия закрытой информации о реальных и потенциальных внешних угрозах его функционированию.

Конечно, цель разведки может быть сформулирована и иным образом, но в любом случае она должна отражать следующие моменты.

Во-первых, своевременность выявления и представления потребителю (т.е. руководству предприятия) необходимой информации (совершенно очевидно, что отсутствие или запаздывание соответствующей информации не позволит принять меры по ликвидации или нейтрализации угроз деятельности предприятия). Во-вторых, необходимо поставлять потребителю не всякую, а качественную информацию. Такой она будет в том случае, если установлены: а) важность (способность внести вклад в деятельность

предприятия); б) точность (надежность источника и самой информации); в) значимость (ценность и правильное понимание информации). В-третьих, сфера действий разведки должна находиться во внешней среде предприятия.

Именно внешняя среда функционирования предприятия является объектом разведывательной деятельности службы безопасности. Она включает в себя [7]:

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

2. Маркетинговых посредников (фирмы, помогающие предприятию в продвижении, сбыте и распространении его товаров среди клиентуры), включающих в себя:

. торговых посредников (деловые фирмы, помогающие компании подыскивать клиентов и/или непосредственно продавать им ее товары);

. фирмы по организации товародвижения (склады, транспортные предприятия и т.д.);

. агентства по оказанию маркетинговых услуг (фирмы маркетинговых исследований, рекламные агентства, организации средств рекламы и консультационные фирмы по маркетингу);

. кредитно-финансовые учреждения (банки, кредитные компании, страховые компании и т.д.).

3. Клиентуру (отдельные лица, приобретающие товары и услуги для личного потребления; организации, приобретающие товары и услуги для использования их в процессе производства; организации, приобретающие товары и услуги для последующей перепродажи их с прибылью для себя; государственные организации, приобретающие товары и услуги либо для последующего их использования в сфере коммунальных услуг, либо для передачи этих товаров и услуг тем, кто в них нуждается; зарубежные потребители, производители, промежуточные продавцы и государственные учреждения).

4. Конкурентов.

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

. финансовые круги (банки, инвестиционные компании, брокерские фирмы, фондовые биржи, акционеры);

. средства массовой информации (газеты, журналы, радиостанции, телецентры и т.д.);

. государственные учреждения, чья деятельность способна отрицательно воздействовать на работу предприятия;

. гражданские группы действий (организации потребителей, экологические объединения, группы, представляющие национальные меньшинства и т.д.);

. местные контактные аудитории (организации самоуправления, преступные группировки, первичные ячейки общественных движений и партий и т.д.).

Достижение цели, поставленной перед разведкой, возможно при реализации следующих задач:

• выявление правонарушений, затрагивающих экономические интересы предприятия;

• своевременное информирование о методах, способах и лицах, имеющих намерение (или исполнивших это намерение) нанести ущерб предприятию и/или его персоналу;

• содействие правоохранительным, судебным и контрольно-надзорным органам в привлечении к ответственности юридических и физических лиц, действия которых затрагивают интересы предприятия-учредителя.

В свою очередь, выполнению этих задач будет способствовать реализация следующих функций [7]:

. изучение негативных и криминальных аспектов теневой экономики и рынка;

. определение степени надежности деловых партнеров; . предоставление руководству предприятия необходимой информации до и во время проведения деловых переговоров;

. выявление предприятий, занимающихся недобросовестной конкуренцией;

. сбор сведений о лицах, не работающих на предприятии и замышляющих либо совершивших преступления против его персонала или/и имущества;

. проверка лиц, заключивших с предприятием коммерческий контракт;

. установление фактов присвоения другими физическими или юридическими лицами утерянного имущества предприятия;

. проверка кредитоспособности деловых партнеров;

. выявление и документирование фактов нарушений прав владельцев товарного знака;

. сбор сведений по гражданским делам в отношении юридических лиц или граждан, ранее не работавших на предприятии;

. выявление среди не работающих на предприятии лиц, занимающихся экономическим шпионажем против предприятия-учредителя. Цели, задачи, функции и другие основные вопросы деятельности разведки обычно отражаются в положениях о разведывательных подразделениях.

Изложенные нами выше соображения о целях, задачах и функциях разведывательного подразделения службы безопасности, если они принимаются, в решающей степени определяют его оргструктуру. В этом случае создается два вида подразделений (отделений, групп, секторов, сотрудников): добывающие и информационные. Основное предназначение добывающих подразделений состоит в добывании всеми доступными и не противоречащими законодательству средствами и методами сведений, документов, предметов и других материалов, которые представляют или могут представить разведывательный интерес. Поэтому в составе этих подразделений должны быть следующие отделения (группы, сектора, отдельные сотрудники): по работе с информаторами; по выявлению и сбору открытых и закрытых публикаций; скрытого наблюдения; технического обеспечения проводимых операций; проведение расследований и документирование поведения изучаемого объекта.

Подразделение контрразведки

Значение и роль контрразведки службы безопасности предприятия в современных условиях жизни обусловлено по крайней мере двумя обстоятельствами: во-первых, стремлением некоторых предпринимателей устранить или нейтрализовать своих конкурентов с помощью средств экономического шпионажа, во-вторых, расширением масштаба криминализации населения, создающей питательную почву для его определенных слоев решать свои потребности преступным путем. Исходя из этого, цель контрразведывательного подразделения можно определить как противодействие разведывательным мероприятиям конкурентов и пресечение правонарушений со стороны противоправных групп или отдельных лиц, посягавших на интересы обслуживаемого предприятия или его отдельных сотрудников.

В отличие от разведки, объектом контрразведывательной деятельности является не внешняя, а внутренняя среда функционирования предприятия. Эта среда включает в себя следующие элементы.

• Руководящий состав предприятия (директор, его заместители, главбух и т.д.) как потенциальные объекты разведывательных мероприятий и/или преступлений со стороны конкурентов.

• Лица из вспомогательного персонала, имеющие доступ к коммерческой тайне (машинистки, работники канцелярии и т.д.).

• Сотрудники, со стороны которых потенциально существует опасность предоставления преступным элементам таких сведений, которые помогут им совершить преступления (сторожа, охранники, водители персональных машин руководителей и т.д.).

• Сотрудники самой службы безопасности.

• Ранее судимые лица из числа работников предприятия.

• Сотрудники предприятия, родственники которых работают у конкурентов.

• Ранее уволившиеся из предприятия его работники.

• Лица, которые в силу своих должностных обязанностей регулярно принимают посетителей предприятия.

Определение цели и объекта контрразведывательной деятельности позволяет определить круг возможных задач подразделения контрразведки:

. борьба с экономическим шпионажем;

. пресечение преступлений против отдельных групп сотрудников (или всех сотрудников на их рабочих местах);

. оказание содействия правоохранительным, судебным и контрольно-надзорным органам в документировании противоправных действий лиц, совершающих уголовные преступления и административные проступки.

Выполнение указанных задач возможно при реализации следующей совокупности функций контрразведки:

. сбор сведений и документов по гражданским и уголовным делам;

. регулярное информирование руководства предприятия о причинах, порождающих совершение правонарушений со стороны персонала и условиях, способствующих этому;

. документирование действий лиц, задержанных за административные проступки;

. выявление лиц из числа персонала, оказывающих содействие преступным элементам (не работающим на предприятии) в совершении ими преступлений;

. информирование руководителей предприятия и телохранителей (если они имеются) о планируемых в отношении их преступлениях;

. поиск без вести пропавших сотрудников предприятия;

. создание условий, исключающих подслушивание разговоров в служебных кабинетах;

. установление обстоятельств разглашения сведений, составляющих коммерческую тайну и др.

Контрольные вопросы

1. Назовите основные задачи подразделения и охраны.
2. Какие требования предусматривает внутриобъектовый режим?
3. Какие требования предусматривает пропускной режим на предприятии?
4. Перечислите виды охранной деятельности.
5. Назовите основные принципы организации режима охраны.
6. Какие функции возлагаются на специальный отдел?
7. Что является источниками конфиденциальной информации на предприятии?
8. Назовите виды конфиденциальной информации, используемой на предприятии.
9. С какой целью на предприятии создается подразделение информационно-аналитической деятельности?
10. Какие мероприятия по защите информации выполняет подразделение инженерно-технической защиты?
11. Дайте характеристику мероприятий по блокированию несанкционированного получения конфиденциальной информации.

12. Зачем на предприятии создаются подразделения разведки?
13. Что является объектом анализа подразделения контрразведки на предприятии?

Глава 6. Организация службы защиты информации (СЗИ)

6.1. Создание СЗИ

Основной задачей службы информационной безопасности является определение направления развития и поддержки усилий организации, направленных на защиту информации от несанкционированного ознакомления, изменения, разрушения или отказа в доступе. Это достигается путем внедрения соответствующих правил, инструкций и указаний [4].

Служба информационной безопасности отвечает:

. за разработку и издание правил (инструкций и указаний) по обеспечению безопасности, соответствующих общим правилам работы организации и требованиям к обработке информации;

. внедрение программы обеспечения безопасности, включая классификацию степени секретности информации (если таковая имеется) и оценку деятельности;

. разработку и обеспечение выполнения программы обучения и ознакомления с основами информационной безопасности в масштабах организации;

. разработку и сопровождение перечня минимальных требований к процедурам контроля за доступом ко всем компьютерным системам, независимо от их размера;

. отбор, внедрение, проверку и эксплуатацию соответствующих методик планирования восстановления работы для всех подразделений организации, принимающих участие в автоматизированной обработке самой важной информации;

. разработку и внедрение процедур пересмотра правил обеспечения информационной безопасности, а также рабочих программ, предназначенных для поддержки правил, инструкций, стандартов и указаний организации;

. участие в описании, конструировании, создании и приобретении систем в целях соблюдения правил безопасности при автоматизации производственных процессов;

. изучение, оценку, выбор и внедрение аппаратных и программных средств, функций и методик обеспечения информационной безопасности, применимых для компьютерных систем организации.

При необходимости на службу информационной безопасности возлагается выполнение других обязанностей:

. формирование требований к системе защиты в процессе создания информационных систем (ИС);

. участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;

. планирование, организация и обеспечение функционирования системы защиты информации в процессе функционирования ИС;

. распределение между пользователями необходимых реквизитов защиты;

. наблюдение за функционированием системы защиты и ее элементов;

. организация проверок надежности функционирования системы защиты;

. обучение пользователей и персонала ИС правилам безопасной обработки информации;

. контроль за соблюдением пользователями и персоналом ИС установленных правил обращения с защищаемой информацией в процессе ее автоматизированной обработки;

. принятие мер при попытках несанкционированного доступа НСД к информации и при нарушениях правил функционирования системы защиты.

При создании СЗИ на предприятии рекомендуется учитывать следующие требования [3]:

• численность службы защиты должна быть достаточной для выполнения всех перечисленных функций;

• служба защиты должна подчиняться тому лицу, которое в данном учреждении несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;

• штатный состав службы защиты не должен иметь других обязанностей, связанных с функционированием ИС;

• сотрудники службы защиты должны иметь право доступа во все помещения, где установлена аппаратура ИС и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;

• руководителю службы защиты должно быть предоставлено право запрещать включение в число действующих новые элементы ИС, если они не отвечают требованиям защиты информации;

• служба защиты информации должна иметь все условия, необходимые для выполнения своих функций.

6.2. Структура СЗИ

В структуру службы безопасности могут входить [7]:

• директор (заместитель директора) или руководитель, непосредственно подчиненный главе фирмы;

• заместитель начальника службы безопасности – на некоторых предприятиях он руководит физической, а иногда и технической службами охраны;

• аналитик;

• юрист;

• специалисты в области обеспечения безопасности, экономической разведки, промышленной контрразведки;

• технические специалисты, умеющие применять специальную технику для защиты помещений;

• сотрудники физической охраны и пропускного режима (по найму), но подчиненные руководителю службы безопасности).

Условно сотрудников службы информационной безопасности можно разделить по функциональным обязанностям [3]:

Сотрудник группы безопасности. В его обязанности входит обеспечение контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема ИС имеет своего сотрудника группы безопасности.

Администратор безопасности системы. В его обязанности входит ежемесячное опубликование нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (при необходимости) и за хранением резервных копий.

Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

Руководитель группы. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах ИС (при децентрализованном управлении).

В небольших организациях функции руководителя службы обычно выполняет либо глава фирмы, либо его заместитель.

Количественный состав службы безопасности различен и зависит, прежде всего, от возможностей самой фирмы. Возможны различные варианты состава такой группы. Кроме того, перечень необходимых знаний и навыков, а также функциональных обязанностей лиц, входящих в группу защиты информации, может существенно отличаться в зависимости от назначения структуры и задач, решаемых в конкретной ИС.

К сожалению, на современном этапе отдается предпочтение физической и технической охране, время "оперативников" и аналитиков только начинается [2].

6.3. Организационно-технические мероприятия СЗИ

Приведем перечень основных организационно-технических мероприятия, выполняемых СЗИ [4]:

. разработка и утверждение функциональных обязанностей должностных лиц службы информационной безопасности;

. внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, обязанности должностных лиц, инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности программно-информационных ресурсов ИС и действиям в случае возникновения кризисных ситуаций;

. оформление юридических документов (договора, приказы и распоряжения руководства организации) по вопросам регламентации отношений с пользователями (клиентами), работающими в автоматизированной системе, между участниками информационного обмена и третьей стороной (арбитраж, третейский суд) о правилах разрешения споров, связанных с применением электронной подписи;

. создание научно-технических и методологических основ защиты ИС;

. исключение возможности тайного проникновения в помещения, установки прослушивающей аппаратуры и т.п.;

. проверка и сертификация используемых в ИС технических и программных средств на предмет определения мер по их защите от утечки по каналам побочных электромагнитных излучений и наводок;

. определение порядка назначения, изменения, утверждения и предоставления конкретным должностным лицам необходимых полномочий по доступу к ресурсам системы;

. разработка правил управления доступом к ресурсам системы, определение перечня задач, решаемых структурными подразделениями организации с использованием ИС, а также используемых при их решении режимов обработки и доступа к данным;

. определение перечня файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требования к уровням их защищенности от НСД при передаче, хранении и обработке в ИС;

. выявление наиболее вероятных угроз для данной ИС, выявление уязвимых мест процесса обработки информации и каналов доступа к ней;

. оценка возможного ущерба, вызванного нарушением безопасности информации, разработка адекватных требований по основным направлениям защиты;

. организация надежного пропускного режима;

. определение порядка-учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;

. организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией;

. организация и контроль за соблюдением всеми должностными лицами требований по обеспечению безопасности обработки информации;

. определение перечня необходимых мер по обеспечению непрерывной работы ИС в критических ситуациях, возникающих в результате НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий и т.п.

. контроль функционирования и управление используемыми средствами защиты;

. явный и скрытый контроль за работой персонала системы;

. контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй и функционирования ИС;

. периодический анализ состояния и оценка эффективности мер защиты информации;

. распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);

. анализ системных журналов, принятие мер по обнаруженным нарушениям правил работы;

. составление правил разграничения доступа пользователей к информации; периодическое с привлечением сторонних специалистов осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты. На основе полученной в результате такого анализа информации принимать необходимые меры по совершенствованию системы защиты;

. рассмотрение и утверждение всех изменений в оборудовании ИС, проверка их на удовлетворение требованиям защиты,документальное отражение изменений и т.п.;

. проверка принимаемых на работу, обучение их правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности.

6.4. Руководитель службы защиты информации

Начальник отдела защиты информации осуществляет в полной мере руководство деятельностью отдела, несет ответственность за надлежащее исполнение возложенных на него обязанностей и обеспечивает:

. исполнение отделом задач и функций, определенных настоящим положением, в соответствии с действующим законодательством и нормативными документами организации;

. обеспечивает соблюдение сотрудниками отдела установленных правил трудового распорядка, производственной и технологической дисциплины;

. разрабатывает и вносит на рассмотрение начальника СБП предложения по совершенствованию структуры отдела и повышению уровня подготовки сотрудников

отдела, улучшение работы и иные предложения по вопросам, входящим в его компетенцию;

. организует техническое обучение и повышение квалификации сотрудников отдела;

. обеспечивает реализацию мероприятий по созданию безопасных условий труда сотрудников отдела на всех технологических участках;

. обеспечивает контроль за соблюдением сотрудниками отдела правил электра и пожарной безопасности;

. распределяет обязанности и разрабатывает должностные инструкции сотрудников отдела;

. представляет сотрудников отдела для назначения или освобождения от должности, поощрения отличившихся работников, наложения дисциплинарных взысканий в соответствии с действующим законодательством о труде и правилами внутреннего трудового распорядка;

. разрабатывает, представляет на утверждение и обеспечивает контроль за порядком доступа в служебные помещения отдела;

. устанавливает регламент проведения профилактических, ремонтных и аварийных работ на установленном в отделе оборудовании;

. координирует совместную деятельность сотрудников отдела со структурными подразделениями службы безопасности и другими подразделениями организации;

. участвует в совещаниях по вопросам информационной безопасности организации и представляет СБП в других учреждениях и организациях по поручению начальника службы безопасности.

Начальник отдела защиты информации отвечает за организацию мероприятий по выполнению требований обеспечения безопасности информации при работе организации. При этом его основными обязанностями являются:

1. Планирование и организация практических мероприятий по предотвращению попыток несанкционированного вмешательства в процесс нормального функционирования ИС и попыток НСД.

2. Организация постоянного контроля за соблюдением сотрудниками организации требований планов защиты конкретных АС и других организационно-распорядительных документов по вопросам обеспечения безопасности информации.

3. Определение особых обязанностей должностных лиц организации по обеспечению безопасности информации при их работе в ИС.

4. Организация проведения занятий с персоналом организации по изучению организационно-распорядительных документов по всему комплексу вопросов обеспечения безопасности информации при работе в ИС.

5. Организация проведения работ по выявлению возможных каналов нарушения информационной безопасности при эксплуатации ИС и принятие своевременных мер по их перекрытию.

6. Организация контроля за выполнением специальных требований по размещению технических средств ИС, прокладке кабельных трасс и инженерных систем, за организацией резервного дублирования и архивирования информации, а также созданием и использованием эталонных копий программного обеспечения по обеспечению безопасности информации и процессов ее обработки.

7. Определение и пересмотр порядка установки и модернизации аппаратных и программных средств ИС организации по обеспечению безопасности информации и процессов ее обработки.

8. Определение и пересмотр порядка проектирования, разработки, отладки, проверки, внедрения и использования программного обеспечения по обеспечению безопасности информации и процессов ее обработки.

Сотрудники отдела защиты информации обязаны [3]:

• проводить практические мероприятия по предотвращению незаконного вмешательства в процесс функционирования системы и несанкционированного доступа (НСД) к информации, обрабатываемой, хранимой и отображаемой на АРМ автоматизированных систем (АС) организации;

• периодически контролировать правильность ведения журналов учета нештатных ситуаций и формуляров автоматизированных рабочих мест в подразделениях организации;

• проводить занятия с сотрудниками подразделений организации по правилам работы на ПЭВМ и по изучению руководящих документов по вопросам обеспечения безопасности информации;

• контролировать выполнение обязанностей администраторами безопасности АС, ответственными за информационную безопасность в подразделениях, ответственных за эксплуатацию конкретных АРМ, обслуживание определенных технических и программных средств;

• участвовать в работе по определению необходимых мер защиты при проектировании программных средств автоматизации решения прикладных задач, по оценке качества реализации необходимых защитных механизмов в АС при испытаниях и внедрении данного программного обеспечения (по обеспечению безопасности информации и процессов ее обработки);

• контролировать исполнение порядка учета, хранения, использования и уничтожения отчуждаемых магнитных носителей конфиденциальной информации;

• контролировать выполнение установленных правил создания, хранения и использования эталонных копий программных средств, соблюдение порядка формирования и использования информационных массивов и баз данных, резервного и архивного копирования данных;

• координировать действия должностных лиц по своевременному восстановлению процесса обработки данных в кризисных (аварийных) ситуациях;

• участвовать в расследовании причин возникновения серьезных кризисных ситуаций;

• постоянно проводить работу по выявлению возможных каналов утечки конфиденциальных сведений при эксплуатации АС и несанкционированного вмешательства в процесс ее функционирования, готовить предложения по совершенствованию системы зашиты и пересмотру плана защиты;

• участвовать в работе комиссий по пересмотру плана защиты АС.

6.5. Разработка должностных инструкций для специалистов по защите информации

При организации службы защиты информации и формировании кадрового состава важным видом работ, как отмечалось в главе 3, является разработка должностных инструкций. В соответствии с общепринятой формой должностной инструкции далее будем рассматривать 4 обязательных раздела:

1 – Общие положения,

2 – Функциональные обязанности,

3 – Права,

4 – Ответственность.

Ранее рассмотренный раздел «Квалификационные требования» на практике обычно включают в раздел 1.

Должностная инструкция подписывается соответствующим специалистом и утверждается директором предприятия.

Ниже приведена «Должностная инструкция инженера по защите информации».

УТВЕРЖДАЮ

_____

(ФИО)

Директор предприятия

_____

(наименование предприятия)

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ИНЖЕНЕРА ПО ЗАЩИТЕ ИНФОРМАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая должностная инструкция определяет функциональные обязанности, права и ответственность инженера по защите информации.

1.2. Инженер по защите информации назначается на должность и освобождается от должности в установленном действующим трудовым законодательством порядке приказом директора предприятия.

1.3. Инженер по защите информации подчиняется непосредственно начальнику службы информационной безопасности (или начальнику СБП).

1.4. На должность инженера по защите информации назначается лицо, имеющее:

1.4.1. Требования к квалификации – высшее профессиональное (техническое) образование без предъявления требований к стажу работы или среднее профессиональное (техническое) образование и стаж работы в должности техника по защите информации I категории не менее 3 лет либо других должностях, замещаемых специалистами со средним профессиональным образованием, не менее 5 лет.

1.5. Инженер по защите информации должен знать:

. постановления, распоряжения, приказы, методические и нормативные материалы по вопросам, связанным с обеспечением технической защиты информации;

. специализацию предприятия и особенности его деятельности;

. методы и средства получения, обработки и передачи информации;

. научно-техническую и другую специальную литературу по техническому обеспечению защиты информации;

. технические средства защиты информации;

. программно-математические средства защиты информации;

. порядок оформления технической документации по защите информации;

. каналы возможной утечки информации;

. методы анализа и защиты информации;

. организацию работ по защите информации;

. инструкции по соблюдению режима проведения специальных работ;

. отечественный и зарубежный опыт в области технической разведки и защиты информации;

. основы экономики, организации производства, труда и управления;

. основы трудового законодательства;

. правила и нормы охраны труда.

1.6. В период временного отсутствия инженера по защите информации его обязанности возлагаются на _____.

2. ФУНКЦИОНАЛЬНЫЕ ОБЯЗАННОСТИ

2.1. Функциональные обязанности Инженера по защите информации определены на основе и в объеме квалификационной характеристики по должности инженера по защите информации и могут быть дополнены, уточнены при подготовке должностной инструкции исходя из конкретных обстоятельств.

2.2. Инженер по защите информации:

2.2.1. Выполняет работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем, проводит исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи.

2.2.2. Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации.

2.2.3. Участвует в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации.

2.2.4. Составляет методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами.

2.2.5. Проводит сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации.

2.2.6. Осуществляет разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации,

принимает участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов.

2.2.7. Составляет информационные обзоры по технической защите информации. Выполняет оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвует в проведении проверок учреждений, организаций и предприятий по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию.

2.2.8. Готовит предложения по заключению соглашений и договоров с другими учреждениями, организациями и предприятиями, предоставляющими услуги в области технических средств защиты информации, составляет заявки на необходимые материалы, оборудование, приборы.

2.2.9. Участвует в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

2.2.10. Проводит контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составляет и оформляет акты контрольных проверок, анализирует результаты проверок и разрабатывает предложения по совершенствованию и повышению эффективности принимаемых мер.

2.2.11. Изучает и обобщает опыт работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны.

2.2.12. Выполняет работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ.

3. ПРАВА

3.1. Инженер по защите информации имеет право:

3.1.1._____.
3.1.2._____.
3.1.3._____.
3.1.4._____.
3.1.5._____.

4. ОТВЕТСТВЕННОСТЬ

4.1. Инженер по защите информации несет ответственность за:

4.1.1. Невыполнение своих функциональных обязанностей.

4.1.2. Недостоверную информацию о состоянии выполнения полученных заданий и поручений, нарушение сроков их исполнения.

4.1.3. Невыполнение приказов, распоряжений директора предприятия, поручений и заданий начальника отдела.

4.1.4. Нарушение Правил внутреннего трудового распорядка, правил противопожарной безопасности и техники безопасности, установленных на предприятии.

5. УСЛОВИЯ РАБОТЫ

5.1. Режим работы инженера по защите информации определяется в соответствии с правилами внутреннего трудового распорядка, установленными на предприятии.

5.2. В связи с производственной необходимостью инженер по защите информации может направляться в служебные командировки (в т.ч. местного значения).

С инструкцией ознакомлен:_____ _____
(подпись) (ФИО)
«____» _____ _____г.

Аналогично составляются и утверждаются должностные инструкции для других категорий специалистов СЗИ.

Контрольные вопросы

1. Перечислите виды деятельности, выполняемые службой информационной безопасности (СЗИ).
2. Кто должен входить в состав СЗИ?
3. Назовите перечень основных организационных технических мероприятий, выполняемых сотрудниками СЗИ.
4. Назовите основные обязанности начальника СЗИ.
5. Что должен выполнять сотрудник СЗИ?
6. На примере должностной инструкции инженера по защите информации опишите четыре обязательных раздела подобных документов.
7. Что должен знать инженер по защите информации?

Лекция №13, №14 4 часа

Глава 7. Управление службой безопасности предприятия (СБП)

7.1 Методы управления СБП
7.2 Функции процессов управления
7.3 Принципы управления СБП
7.4 Виды обеспечения деятельности СБП
7.5 Управление безопасностью предприятия в кризисных ситуациях

7.1. Методы управления СБП

Основной целью деятельности СБП является своевременное пересечение (нейтрализация) противоправных посягательств на экономические интересы, персонал предприятия, предотвращение материального и физического вреда, а также предотвращение и пресечение преступлений, административных проступков и гражданско-правовых конфликтов и т.д.

Формулирование цели управления зависит от многих факторов: финансовых возможностей предприятия-учредителя, его географического месторасположения, возможности набрать из числа жителей данной территории квалифицированный состав сотрудников службы безопасности и т.д.

На основе сформулированной цели проектируется и создается оргструктура службы безопасности. Анализ изученных документов служб безопасности свидетельствует, что наибольшее распространение получили линейная и линейно-штабная структура. Линейная структура характеризуется четким единоначалием – каждый сотрудник подчинен только одному вышестоящему лицу.

Линейно-штабная структура представляет собой линейную структуру, дополненную штабным органом (штабом), на который возлагаются дополнительные функции управления. Такая структура создается обычно тогда, когда большое количество сотрудников или их территориальная разобщенность не позволяют начальнику службы безопасности эффективно управлять [7].

Эффективное функционирование службы безопасности предполагает предварительную проработку многих вопросов. Среди них особое значение приобретает проектирование оргструктуры службы безопасности и ее ресурсного обеспечения, т.к. без решения этих вопросов ее деятельность вообще невозможна. Собственно говоря, употребляемый нами многозначный термин «организация» среди многих значений имеет и такое, как создание нужной структуры и необходимых ресурсов.

Общеизвестно, что любое оргструктурное формирование создается для реализации определенных функций. Применительно к службе безопасности предприятия эти функции определены ст. 3 закона РФ «О частной детективной и охранной деятельности в Российской Федерации».

Этим законом (ст.14) предусмотрена должность руководителя службы безопасности, которая на практике реализуется в виде начальника службы безопасности (здесь сказался прошлый опыт деятельности в правоохранительных органах персонала службы безопасности). Совершенно очевидно, что если персонал службы безопасности по количеству большой, неизбежно встает вопрос о заместителях начальника службы безопасности. Их может быть несколько (обычно по количеству подразделений службы безопасности).

Как правило, заместитель начальника службы безопасности является одновременно руководителем одного из подразделении и, в свою очередь, также имеет одного или нескольких заместителей. Не вызывает сомнений целесообразность создания таких подразделений, как канцелярия и бухгалтерия (в случае, если службу безопасности не обслуживает единая бухгалтерия предприятия-учредителя).

В крупных службах безопасности, где возникает необходимость создания штабных подразделений, так как начальники службы безопасности просто физически не способны на должном уровне выполнять такие управленческие функции, как анализ, планирование, контроль и т.д., исполнение этих обязанностей помощниками положение дел не меняет, так как в этом случае возникает необходимость их повседневного руководства, что опять-таки не под силу начальнику службы безопасности, и он вынужден будет назначить одного из них координатором деятельности других, а это, по сути, означает выполнение обязанностей начальника штаба.

Предложенная схема оргструктуры может время от времени уточняться и пересматриваться.

Любая оргструктура, даже самая оптимальная, не сможет дать ожидаемых результатов, если ее не дополнить внутренними нормативными актами, регулирующими деятельность всех подразделений и сотрудников службы безопасности. Образно выражаясь, «кость» (оргструктура) должна обрасти «мясом» (нормативными документами). Причем эти нормативные акты условно можно разделить на две группы: непосредственно относящиеся к деятельности самой службы безопасности и к деятельности других служб (подразделений, сотрудников) предприятия [7].

Методы управления службой безопасности подразделяются на три группы:

1) экономические;

2) организационно-распорядительные;

3) социально-психологические.

Руководители службы безопасности должны безупречно владеть всеми методами управления в их единстве. Для этого они должны знать особенности каждого из них. Экономические методы управления строятся на использовании различных экономических стимулов, таких, например, как заработная плата. Умелое использование этого стимула с учетом уровня профессионализма, стажа работы, результатов деятельности сотрудника и т.д. позволяет эффективно организовать работу отдельных сотрудников в рамках службы безопасности.

Организационно-распорядительные методы управления (приказы, распоряжения, указания, инструкции и т.д.) подразделяются на три группы: распорядительные, организационно-стабилизирующие и дисциплинирующие. Особое внимание в деятельности службы безопасности следует уделить таким нормативам (производные от организационно-стабилизирующих методов) как нормативы времени выполнения той или иной деятельности, численности сотрудников того или иного подразделения и т.д. Такие нормативы обычно перенимаются из опыта работы органов внутренних дел, ФСБ и т.д., с поправкой на специфику деятельности службы безопасности предприятия, фирмы.

Социально-психологические методы основаны на использовании моральных стимулов к труду и воздействуют на личность сотрудника службы безопасности с помощью психологических приемов с целью превращения задания в осознанный долг, внутреннюю потребность человека. Это достигается посредством приемов, которые носят личностный характер (личный пример, авторитет и т.д.). На уровне коллектива службы безопасности действуют методы, включающие оценку индивидуальных качеств сотрудников и выработку ориентиров, создающих условия для максимального проявления их профессиональных качеств.

Структура процесса управления в самом общем виде состоит из трех стадий, каждая из которых включает в себя последовательно осуществляемые этапы или операции:

I стадия. Сбор, обработка, обобщение и анализ информации

II стадия. Выработка и принятие управленческого решения.

III стадия. Организация исполнения управленческого решения.

При разработке управленческих подходов для решения конкретных вопросов по предотвращению различных угроз необходимо учитывать различные режимы функционирования СПБ.

На рис. 7.1. приведена общая схема организации работ в условиях повседневной деятельности, повышенной готовности и при чрезвычайном положении (кризисной ситуации).

7.2. Функции процессов управления СБП

При рассмотрении основных процессов управления в современной теории менеджмента выделяют 4 типовых функции:

- планирование;
- организация;
- мотивация;
- контроль;

и два связывающего их процесса: коммуникации и принятия решения, подробно рассмотренные в работе [1].

Р Е Ж И М Ы

Подпись: Рис. 7.1. Режимы функционирования СБП

Применительно к рассматриваемому объекту управления СПБ, по мнению В.П. Мак-Мака [7], целесообразно выделять шесть функций:

- Прогнозирование.
- Планирование.
- Организация.
- Регулирование.
- Мотивация.
- Контроль.

В системе управления все эти функции должны быть объединены в целостный процесс, хотя из методических соображений целесообразно рассматривать их отдельно. Рассмотрим далее указанные функции с учетом специфики деятельности службы безопасности.

Прогнозирование предполагает составление заключения (прогноза) о будущих событиях и тенденциях развития службы безопасности. Прогнозные оценки бывают оперативными (с упреждением не более одного месяца), краткосрочными (от 1 месяца до 1 года), среднесрочными (от 1 года до 5 лет). Составляются они как привлеченными со стороны специалистами, так и сотрудниками службы безопасности (в первую очередь сотрудниками штаба).

Качество прогнозных оценок повышается, если они составляются сотрудниками службы безопасности с помощью приглашенных экспертов-специалистов в той или иной области. Представляется, что наиболее целесообразным было бы составление следующих видов прогнозных оценок:

- криминологических;
- рисковых (коммерческий, финансовый и т.д.) в предпринимательской деятельности;
- экономических, физических, информационных и т.д., определяющих безопасность предприятия.

Так, в работе [7] описан набор признаков, свидетельствующих о возможных условиях для реализации преступного замысла в отношении охраняемого объекта:

1. Выявление на объекте или на прилегающей территории тайников, приспособленных преступниками для сохранения похищенного; приспособлений, с помощью которых можно проникнуть на объект; смесей, отбивающих у собаки желание работать и т.д.
2. Обнаружение охраной или сотрудниками объекта подготовленных, но замаскированных мест возможного проникновения на объект, например в районе

прохождения коммуникаций через капитальные перекрытия и стены, возле длительное время неиспользуемых «черных» ходов и запасных выходов с объекта.

3. Обнаружение оторванных и приставленных к забору досок, выпиленных или выдолбленных камней, кирпичей или плит в ограждении или стене объекта.

4. Информация о случаях кражи с объектов дефицитного портативного газосварочного оборудования, а также установленные службой безопасности факты приобретения такого рода оборудования лицами с сомнительным прошлым, ранее судимыми, теми, о ком имеется информация, подтверждающая их связь с преступным миром.

5. Информация об участившихся встречах криминальных элементов с бывшими сотрудниками фирмы или ее охраны.

6. Факты краж или нападений преступников на конструктивно схожие объекты, но не охраняемые.

7. Факты угроз в адрес собственника объекта, которые могут быть как бы последней попыткой склонения фирмы (ее руководителя) к выплате определенного процента от прибыли преступникам.

8. Фиксируемые охраной факты появления возле объекта лиц, действия которых напоминают тренировочные занятия по ознакомлению с местностью, проникновению на объект или по обработке иных специальных навыков и приемов.

9. Случаи «хулиганского» разбивания стекол на объекте, стуков в двери и окна, телефонные звонки от имени людей, «ошибшихся» номером.

10. Участившиеся случаи задержания посторонних на территории объекта, а также попытки неизвестных лиц проникнуть на территорию объекта без определенных намерений.

11. Обнаружение охраной внутри объекта переброшенных снаружи мотков проволоки, досок, крупных камней, которые могут использоваться преступниками для провоцирования срабатывания сигнализации и отвлечения охраны.

12. Случаи возникновения драк и хулиганских проявлений возле объекта, повреждение автомашины сотрудников охраны, факты неожиданного отключения света на объекте.

13. Попытки криминальных элементов устроиться на работу в фирму.

14. Возникновение повышенного интереса и внимания к фирме со стороны коммерческих структур непосредственно перед прибытием на объект ценных грузов (если это обстоятельство ранее не рекламировалось).

15. Признаки возможной связи сотрудников фирмы с криминальными элементами.

Планирование предполагает определение целей, задач службы безопасности на предстоящий период деятельности, средств и времени на их достижение. Наиболее распространенными в деятельности служб безопасности являются комплексные и специальные планы.

Комплексные планы охватывают все сферы деятельности службы безопасности и включают в себя, как правило, такие разделы, как организационные вопросы обеспечения всех видов безопасности предприятия (в рамках компетенции службы безопасности), работу с кадрами, ресурсное обеспечение, контроль и т.д. Наиболее приемлемая форма составления такого плана имеет следующий вид:

№ п/п

Содержание планируемого мероприятия

Срок исп.

Ответств. за исп.

Форма представления результатов выполненного мероприятия

Отметка об исполнении

I

II
III
IV
V
VI

Существуют и другие подходы к формированию комплексных планов. Так, в работе [7] предлагается следующая структура основных разделов плана организации системы безопасности и защиты предприятия:

1. Задачи службы безопасности.

2. Выводы и оценки обстановки:

а) положение на рынке услуг (производство);

б) основные группировки сил конкурентов, преступных элементов (их построение, способы действий, возможности);

в) основные угрозы предприятию;

г) силы СБП, ее состав, возможности:

д) особенности ситуации в стране, городе (месте дислокации фирмы) и ее влияние на рынок услуг и производства.

3. Задачи, решаемые службами безопасности соседних предприятий в интересах предприятия.

4. Задачи, решаемые силами и средствами МВД в интересах предприятия.

5. Указания по взаимодействию с МВД и другими службами безопасности.

6. Организация развертывания и усиления сил СБП, техническое и материальное обеспечение их деятельности.

7. Указание (план) по организации управления силами СБП в экстремальных ситуациях (по вариантам).

8. Срок готовности сил к выполнению функциональных обязанностей в полном объеме.

Не отрицая возможности такой структуры плана, отметим, что его реализация требует согласования с органами внутренних дел и службами безопасности соседних предприятий, что в современных условиях маловероятно.

Специальные планы разрабатываются на случай возникновения чрезвычайных происшествий и чрезвычайных ситуаций (нападения на объект, угроза взрыва бомбы, захват заложников, наводнение, пожар и т.д.).

Организация – как функция состоит в установлении постоянных и временных взаимоотношений между всеми подразделениями службы безопасности, определение порядка и условий ее функционирования. Это процесс включает в себя следующие элементы:

1. Определение рациональных форм разделения труда. В сфере управления существует следующее технологическое разделение труда: технические исполнители (секретари, машинистки, операторы ЭВМ), специалисты (юристы, аналитики и т.д.) и руководители службы безопасности и его подразделений.

2.Распределение работ среди работников, групп работников. В первую очередь, такое обязательное распределение происходит между такими группами работников, как детективы и охранники (в рамках соответствующих подразделений). Во вторую очередь, работа распределяется между отделениями, секторами и группами, являющимися структурными единицами подразделений (отделов) службы безопасности. И лишь в третью очередь, работа распределяется между самими работниками. Материальное выражение такого распределения работ находит в разработке положений о подразделениях, его структурных единицах и должностных инструкциях.

3. Разработка структуры органов управления. В службе безопасности орган управления состоит из трех уровней. Высший уровень представлен начальником службы безопасности и его заместителем. Эта группа управленческих работников обеспечивает интересы и потребности руководителей предприятия-учредителя, вырабатывает политику службы безопасности и способствует ее практической реализации. Руководители среднего уровня управления (начальники подразделений) обеспечивают реализацию политики функционирования службы безопасности, разработанной высшим руководством, и отвечают за доведение более детальных заданий до своих подчиненных, а также за их выполнение. Низший уровень управления представлен младшими руководителями (начальниками отделений, групп, секторов), которые отвечают за доведение конкретных заданий до непосредственных исполнителей, а также за их выполнение.

4.Регламентация функций, подфункций, работ, операций. Такую регламентацию следует проводить, начиная последовательно с функций и заканчивая операциями. Отражать их необходимо в уставе, положениях об отделах, отделениях, группах и секторах (функции), должностных и служебных инструкциях (работы, операции). При этом очень важно обеспечить эту регламентацию таким образом, чтобы соблюдалась определенная соподчиненность между функциями, подфункциями, работами и операциями.

5. Установление прав и обязанностей органов управления и их сотрудников. Правами и обязанностями наделяются как структурные подразделения службы безопасности, так и её сотрудники. При этом важно таким образом установить обязанности, чтобы для их реализации были предоставлены соответствующие права (совпадение объема прав и обязанностей). Отражаются права и обязанности в уставе службы безопасности, положениях и должностных инструкциях. Следует при этом избегать отождествления прав и обязанностей сотрудников с правами и обязанностями службы безопасности и подразделений.

6. Подбор и расстановка кадров. Подбор кандидатов для работы в службе безопасности происходит в соответствии с требованиями, предусмотренными в законе «О частной детективной и охранной деятельности в Российской Федерации». Но в отличие от процедуры подбора кадров, где практически все вопросы жестко регламентированы, руководителям службы безопасности предоставлены определенные возможности в расстановке кадров. Такая расстановка возможна как по горизонтали, так и по вертикали.

Регулирование представляет собой «наладку» системы, приведение ее в нормальное рабочее состояние и необходимость в ней возникает в силу изменения внешних условий либо из-за возникновения каких-то нарушений, «сбоев» в функционировании самой системы. Посредством этой функции достигается поддержание управляемых процессов в рамках, заданных программой, регламентом, планом. Орган управления службы безопасности через эту функцию должен обеспечить сохранение заданных параметров следующими приемами:

А. Выравнивание отклонений. Так, если в сравнении с аналогичным периодом прошлого года резко возросло количество краж с охраняемого объекта, то проводится комплекс мероприятий по значительному их снижению (профилактические беседы, рейды, операции и т.д.). В результате применения этого приема управляемая подсистема приводится к некой норме, удовлетворяющей руководство службы безопасности и предприятия-учредителя.

Б. Компенсация возмущений. Возмущающее воздействие внешней среды на деятельность сотрудников службы безопасности выражается иногда в отрицательном воздействии на их поведение. Такое воздействие может выражаться, например, в отказе руководства повысить им зарплату в условиях высокой инфляции, резком увеличении нагрузки и т.д. В таком случае необходимо включить так называемые компенсаторные механизмы, к примеру предоставить сотрудникам ряд материальных льгот (бесплатные

питание и проезд в общественном транспорте и т.д.), увеличить количество отгулов и т.д. Реакция на возмущающее воздействие должна быть своевременной и эффективной.

В. Устранение воздействия помех. Помехи в деятельности службы безопасности могут быть как естественные (землетрясения, наводнения и т.д.), так искусственные (нападения на охраняемый объект, дискредитация руководства предприятия в средствах массовой информации, поджоги помещений и т.д.). Необходимо предварительно составить перечень (каталог) таких возможных помех и отработать систему.

Мотивация – это процесс побуждения сотрудников службы безопасности к деятельности для достижения целей самой службы и ее подразделений. Мотивация представляет собой совокупность сил, побуждающих сотрудника осуществлять деятельность с затратой определенных усилий, на определенном уровне старания и добросовестности, с определенной степенью настойчивости в направлении достижения определенных целей.

В основе любой теории мотивации лежат потребности человека, которые можно удовлетворить вознаграждениями. Причем выделяют внешние вознаграждения (заработная плата, премии и т.д.) и внутренние – чувство успеха при достижении цели, получаемое от самой работы.

Для практических целей достаточна типология с использованием трех типов мотивации: I тип - сотрудники, ориентированные преимущественно на содержательность и общественную значимость труда; II тип - преимущественно ориентированные на оплату труда и другие нетрудовые ценности; III тип - сотрудники, у которых значимость разных ценностей сбалансирована.

Среди потребностей, которые обладают конкретными мотивационно-трудовыми значениями, можно выделить следующие:

• потребность в самоуважении (добросовестная трудовая деятельность независимо от контроля и оплаты труда ради положительного собственного мнения о себе как о человеке и работнике);

• потребность в самоутверждении (высокие количественные и качественные показатели в труде ради одобрения и авторитета, похвалы, положительное отношение со стороны коллектива и руководства);

• потребность в признании (направленность трудового поведения на доказательство своей профессиональной пригодности и способностей);

• потребность в самовыражении (высокие показатели в работе основе творческого отношения к ней);

• потребность в активности (трудовая деятельность как самоцель, стремление к поддержанию через активность здоровья и самочувствия целостности личности);

• потребность в стабильности (восприятие работы как способа поддержания существующего образа жизни, достигнутого достатка);

• потребность в общении (установка на трудовую деятельность вообще и частные фрагменты работы как условия и повод для человеческих контактов и знакомств; хорошая работа как основа и тема общения).

Перечисленные моральные потребности как мотивы к труду не могут заменить собой материальные планы и ожидания. Вот почему руководители службы безопасности должны использовать в своей деятельности все формы материального и морального стимулирования своих подчиненных, добиваясь высокой мотивации их труда.

Контроль состоит в процессе соизмерения (сопоставления) фактически достигнутых результатов с запланированными. Эффективная система контроля должна соответствовать следующим требованиям:

а) контроль должен быть всеобъемлющим;

б) контроль следует сосредоточить на результате;

в) система контроля должна быть простой;

г) контроль не может быть ни целенаправленным, ни нейтральным;

д) контроль должен быть постоянным.

Субъектами контрольной деятельности в службе безопасности являются руководитель предприятия-учредителя, члены совета (комитета) безопасности предприятия, руководители службы безопасности и его подразделений (в рамках своей компетенции). Кроме этого, внешними субъектами контроля могут быть сотрудники лицензионно-разрешительных подразделений органов внутренних дел и прокуратуры.

Подконтрольными объектами могут быть деятельность подразделений, состояние технической укрепленности охраняемого объекта, защищенность коммерческой тайны, система профессиональной подготовки и переподготовки сотрудников службы безопасности и т.д. Выбор объекта контроля определяется его способностью влиять (положительно или отрицательно) на деятельность службы безопасности в целом. В рамках подконтрольного объекта очень важны его составные элементы, после определения которых можно непосредственно приступить к контролю. Так, в рамках проверки состояния защиты коммерческой тайны на предприятии должны быть изучены:

1) соблюдение норм, правил хранения и охраны в помещениях, спецхранилищах, на рабочих местах носителей информации;

2) ведение учета и обеспечение личной ответственности за выполнение данной функции;

3) соблюдение порядка хранения и уничтожения засекреченных сведений;

4) соблюдение требований порядка обращения с носителями коммерческой тайны;

5) меры по предотвращению несанкционированного выноса носителей коммерческой тайны за территорию предприятия.

7.3. Принципы управления СБП

Принципы управления службой безопасности определяют требования к системе структуре и организации процесса управления. В рамках службы безопасности это следующие принципы [7]:

1. Научность. Основное содержание этого принципа заключается в требовании, чтобы все управленческие действия осуществлялись на базе применения научных методов и подходов. Между прочим, этот принцип требует от руководителей службы безопасности и его подразделений внимательного изучения управленческой и специальной литературы по проблемам обеспечения безопасности предприятия.

2. Единоналичие и коллегиальность. Сущность этого принципа заключается в том, что на основе мнений низовых руководителей и рядовых исполнителей конкретных решений, вышестоящий начальник пользуется правом единоличного решения вопросов, входящих в его компетенцию.

3. Принцип системности и комплексности. Системность означает необходимость использования элементов теории больших систем, системного анализа в каждом управленческом решении. Комплексность в управлении означает необходимость всестороннего охвата управляемой системы, учета всех сторон, всех направлений, всех свойств. Этот принцип требует от руководителей службы безопасности выработки у себя аналитико-синтетического склада мышления.

4. Принцип системности и комплексности. Этот принцип состоит в оптимальном распределении (делегировании) полномочий при принятии управленческих решений. Здесь следует руководствоваться таким правилом: тот, кому предстоит выполнять управленческое решение, должен его самостоятельно разработать и, с учетом возможных корректив вышестоящего руководства, активно добиваться его реализации.

5. Принцип плановости. Сущность этого принципа состоит в установлении основных направлений и пропорций службы безопасности в перспективе. Практическая

реализация этого принципа означает, что все сотрудники, подразделения и службы безопасности в целом должны планировать свою деятельность в такой последовательности: служба безопасности - подразделения - сотрудник.

6. Принцип сочетания прав, обязанностей и ответственности. Этот принцип предполагает, что каждый сотрудник службы безопасности должен выполнять возложенные на него обязанности, при этом он наделяется адекватными ему правами и несет ответственность за качество их выполнения.

7.4. Обеспечение деятельности службы безопасности

Для успешного функционирования и эффективного управления службой безопасности необходимо обеспечить ее материально-техническими, финансовыми, кадровыми и информационными ресурсами [11].

Среди них первостепенное значение имеют финансовые ресурсы. Без финансового обеспечения деятельности службы безопасности бессмысленно вообще говорить о ее функционировании.

Поскольку служба безопасности не вправе самостоятельно зарабатывать деньги путем заключения договоров с другими клиентами, именно на предприятии-учредителе лежит обязанность финансирования ее деятельности. Но это не означает, что руководство службы безопасности должно занимать в этом вопросе пассивную позицию. Напротив, обоснованные текущие и прогнозные оценки в финансовых потребностях службы безопасности и основанные на них точные расчеты должны стать правилом, а не исключением. Финансовую политику службы безопасности определяют, конечно, ее руководители, но при этом активную помощь им должна оказывать бухгалтерская служба.

В функции этой службы входит ведение табеля, учета рабочего времени; начисление зарплаты, премий и т.д.; учет выплат за различные услуги; перечисление денег; выдача сотрудникам их денежного содержания; оплата счетов и т.д. Поскольку руководители службы безопасности не являются, как правило, специалистами в финансовых вопросах, наиболее целесообразно свое внимание сосредоточить им на некоторых ключевых моментах.

Во-первых, периодически проверять финансовое состояние службы безопасности с помощью приглашенных специалистов. Во-вторых, открывать расчетные и текущие счета только в надежных банках. В-третьих, добиваться такого уровня минимальной зарплаты персонала службы безопасности, чтобы у него не возникало соблазна увольняться (можно порекомендовать в связи с этим устанавливать в контрактах сумму зарплаты в иностранной валюте по курсу Центрального банка России на день его выдачи). В-четвертых, установить поэтапное финансирование закупленных (приобретенных) материально-технических средств от наиболее необходимых (например, в первую очередь, оружие, спецсредства) до менее необходимых (например, канцелярские принадлежности и т.д.). Наконец, рационально и обоснованно использовать деньги из фонда поощрения и материальной помощи персоналу [7].

Полное и качественное обеспечение деятельности службы безопасности материально-техническими ресурсами - не только средство, но и условие повышения эффективности работы его сотрудников Эти ресурсы условно подразделяются на следующие группы:

• оружие и боеприпасы;

• специальные средства;

• служебные помещения различного характера (кабинеты, караульные помещения, оружейные комнаты, стрелковые тиры, комнаты досмотра);

• вспомогательная техника (автотранспорт, видео, -кино, -фототехника, средства оперативной радио- и телефонной связи, компьютеры и т.д.);

• средства предупреждения и защиты (охранно-пожарная сигнализация, сторожевые собаки, охранное освещение, телевидение т.д.);

• средства обеспечения нормальной деятельности сотрудников (форменное обмундирование, мебель, канцелярские принадлежности, медикаменты, бланки документов, юридическая и специальная литература и т.д.).

Обеспечение оружием, боеприпасами, спецсредствами сотрудников службы безопасности регламентировано законом и нормативными актами правительства, МВД и Министерства финансов России. В отношении обеспечения некоторых средств целесообразно использовать нормативы, имеющиеся в различных министерствах и ведомствах (количество служебных собак, оборудование и размеры стрелкового тира, наличие медикаментов, расчет различных видов охранно-пожарной сигнализации и т.д.).

Наконец, последнее по счету, но не по важности, обеспечение деятельности службы безопасности информационными ресурсами.

Прежде всего, следует определить потребность и объемы минимума информации, без которых функционирование службы безопасности вообще невозможно. Такую информацию можно условно разделить на три блока («Среда функционирования предприятия», «Состояние безопасности внутри предприятия» и «Внутриорганизационная деятельность службы безопасности»), после чего в рамках каждого блока разработать перечень необходимых сведений. Этот перечень не будет носить произвольный характер, если при его составлении руководствоваться одним принципом: любая информация реально должна «обслуживать», «работать» на реализацию, как минимум, одной функции службы безопасности. Можно рекомендовать в этой связи включать в указанные блоки следующие сведения, которые, разумеется, не могут быть исчерпывающими [7].

В 1-й блок «Среда функционирования предприятия» возможно включение сведений о предприятиях-конкурентах, правоохранительных и контрольно-надзорных органах, рыночной конъюнктуре, криминогенной ситуации в районе месторасположения предприятия, нормативных актах, регулирующих деятельность предприятия-учредителя и т.д.

Во 2-й блок «Состояние безопасности внутри предприятия» целесообразно включить следующие сведения: состояние преступности среди персонала, наличие или отсутствие коммерческой тайны, источники (каналы) и суммы материального ущерба, наносимого предприятию, анализ насильственных преступлений, совершенных против его персонала, эффективность работы юрисконсульта (юридической службы), о сотрудниках предприятия, имеющих доступ к конфиденциальной информации, с корыстно-насильственной мотивацией, связанных с сохранностью товарно-материальных ценностей; местонахождении и правилах работы с документацией, содержащей коммерческую тайну; месторасположении и состоянии сохранности изделий (описания процесса), составляющих секрет предприятия и т.д.

Наконец, в 3-м блоке «Внутриорганизационная деятельность службы безопасности» желательно иметь сведения о составе и структуре службы безопасности, перемещениях сотрудников, дисциплинарной практике, результатах проверок, состоянии законности и т.д.

Совершенно очевидно, что без надлежащей организации такого массива информации, удобной и практичной для использования, не обойтись. Идеальным вариантом в этом случае было бы создание информационной системы на базе компьютерной техники, однако его создание требует определенных финансовых затрат. Поэтому на практике чаще всего встречается отражение и систематизация необходимой информации в письменных документах. К документам, составляемым в службе безопасности, относятся:

. организационные документы (устав, положение, должностные инструкции, штатное расписание, правила внутреннего трудового распорядка);

. правовые документы (законы, подзаконные акты, методические рекомендации по проблемам безопасности и т.д.);

. распорядительные документы (приказы, инструкции, указания, графики работы персонала и т.д.);

. информационно-справочные документы (протоколы, акты, справки, письма, докладные и объяснительные записки, телефонограммы, телеграммы, досье и т.д.);

. договоры, трудовые соглашения;

. документы по личному составу (приказы по личному составу, трудовые книжки, материалы проверок по жалобам, графики отпусков и т.д.).

В результате правильно организованного документального отражения необходимых сведений достигается эффективное информационное обеспечение деятельности службы безопасности.

Не менее важное значение для руководителей службы безопасности имеет вопрос кадрового обеспечения ее деятельности. Работу эту условно можно разделить на два этапа.

На первом этапе происходит отбор кандидатов для работы в службе безопасности, их проверка, прохождение ими специальной подготовки и стажировка в должности. При отборе кандидатов особое внимание должно уделяться их образованию (помимо юристов, целесообразно приглашать на работу экономистов, финансистов и в последнее время специалистов по защите информации). Помимо проверки через органы внутренних дел, проводится дополнительное выяснение биографических и других характеризующих личность кандидата данных. Разумеется, это необходимо делать не во всех случаях (излишней будет такая проверка, например, кандидата, которого хорошо и давно знает руководитель службы безопасности) и с письменного согласия кандидатов. Однако письменное согласие на проверку такого рода после зачисления кандидата в службе безопасности необходимо получать в любом случае.

Если в процессе проверки установлена пригодность кандидата для работы в службе безопасности, то его направляют на учебу в негосударственное образовательное учреждение (за исключением лиц, имеющих стаж работы в оперативных или следственных подразделениях не менее трех лет). При этом особое внимание обращается на наличие лицензии у этого учреждения и качество программы обучения. После прохождения специальной подготовки и получения лицензии охранника или детектива целесообразно организовать стажировку его в соответствующей должности (от 1 до 6 мес.) и лишь после этого решать вопрос об его зачислении на постоянную работу в службе безопасности или увольнении. Разумеется, такая возможность должна быть предусмотрена в контракте, который подписывается после отбора кандидата.

7.5. Управление безопасностью предприятия в кризисных ситуациях

Служба безопасности должна быть всегда готова к возникновению критических (кризисных) ситуаций, проявляющихся в результате столкновения интересов бизнеса и преступного мира.

Кризисная ситуация – это проявление фактов угроз со стороны отдельных лиц или групп. Кризисная ситуация может проявляться и развиваться по-разному: медленно или спонтанно, мгновенно [13].

При оценке и анализе кризисной ситуации очень важно как можно быстрее определиться с ответом на вопрос, способна ли СБП справиться с ситуацией своими силами либо для ее разрешения необходимо привлечение правоохранительных органов. Однако в любом случае, учитывая возможность возникновения кризисных ситуаций, любая фирма стремится создать в составе СБП отдельное формирование, именуемое КРИЗИСНАЯ ГРУППА. Она создается из числа ключевых фигур фирмы: директор,

руководители линейных подразделений, филиалов, служб, юрист, главный бухгалтер и др. Кризисная группа может быть создана на постоянной основе с непременным включением в число ее членов:

• руководителя фирмы;
• юриста;
• финансиста;
• руководителя службы безопасности.

Руководство кризисной группой может быть возложено на главу фирмы. Перечисленные лица, как правило, в силу своего служебного положения, обладания специальными знаниями, опытом располагают реальными возможностями достаточно эффективно воздействовать на обстоятельства, в условиях которых возникает и протекает кризисная ситуация, не выпуская при этом рычагов влияния на повседневную коммерческую и производственную деятельность.

В каждом конкретном случае в состав кризисной группы могут включаться и иные специалисты.

Кризисная группа решает следующие задачи:

. оценка обстановки;
. принятие неотложных мер по безопасности;
. управление деятельностью фирмы в экстренных условиях;
. обеспечение оперативного взаимодействия с органами правопорядка.

Главная цель создания кризисной группы – противодействие внешним угрозам безопасности фирмы. Рабочие заседания группы должны проходить в условиях предельной конфиденциальности. Как правило, деятельность кризисной группы регламентируется типовым планом действий руководства и персонала фирмы. В зависимости от складывающейся ситуации планы могут быть следующего вида, а именно, план действий:

. при угрозе взрыва;
. захвате заложников или похищении сотрудников фирмы;
. вымогательстве;
. нападении на помещения фирмы;
. нападении на инкассаторов.

Типовые кризисные планы являются документами конфиденциального характера, доступ к которым должен иметь узкий круг лиц. Составляться подобные планы должны не более чем в двух-трех экземплярах. Один хранится у руководителя, другой – у начальника службы безопасности, третий может находиться у лица, замещающего руководителя фирмы в его отсутствие.

Осуществляя планирование, надо исходить из того, что план – это не набор мероприятий, а последовательная линия поведения, стратегия деятельности фирмы в конкретной кризисной ситуации, направленная на обеспечение эффективной безопасности.

Контрольные вопросы

1. Назовите три группы методов управления службой безопасности.
2. Какие функции рассматриваются при управлении СБП?
3. В чем выражается прогнозирование ситуации со стороны сотрудников СБП?
4. Какие разделы включают в план при организации системы безопасности?
5. Что включает в себя функция «организации» при управлении СБП?

6. Перечислите основные потребности сотрудников, используемые для их мотивации в условиях управления СБП.

7. Кто и кого должен контролировать при управлении СБП?

8. Перечислите принципы управления СБП.

9. Назовите четыре вида обеспечения деятельности СБП.

10. Чем отличается управление СБП в крупной ситуации от обычного режима работы?

Глава 7. Управление службой безопасности предприятия (СБП)

7.1. Методы управления СБП

Основной целью деятельности СБП является своевременное пересечение (нейтрализация) противоправных посягательств на экономические интересы, персонал предприятия, предотвращение материального и физического вреда, а также предотвращение и пресечение преступлений, административных проступков и гражданско-правовых конфликтов и т.д.

Формулирование цели управления зависит от многих факторов: финансовых возможностей предприятия-учредителя, его географического месторасположения, возможности набрать из числа жителей данной территории квалифицированный состав сотрудников службы безопасности и т.д.

На основе сформулированной цели проектируется и создается оргструктура службы безопасности. Анализ изученных документов служб безопасности свидетельствует, что наибольшее распространение получили линейная и линейно-штабная структура. Линейная структура характеризуется четким единоначалием – каждый сотрудник подчинен только одному вышестоящему лицу.

Линейно-штабная структура представляет собой линейную структуру, дополненную штабным органом (штабом), на который возлагаются дополнительные функции управления. Такая структура создается обычно тогда, когда большое количество сотрудников или их территориальная разобщенность не позволяют начальнику службы безопасности эффективно управлять [7].

Эффективное функционирование службы безопасности предполагает предварительную проработку многих вопросов. Среди них особое значение приобретает проектирование оргструктуры службы безопасности и ее ресурсного обеспечения, т.к. без решения этих вопросов ее деятельность вообще невозможна. Собственно говоря, употребляемый нами многозначный термин «организация» среди многих значений имеет и такое, как создание нужной структуры и необходимых ресурсов.

Общеизвестно, что любое оргструктурное формирование создается для реализации определенных функций. Применительно к службе безопасности предприятия эти функции определены ст. 3 закона РФ «О частной детективной и охранной деятельности в Российской Федерации».

Этим законом (ст.14) предусмотрена должность руководителя службы безопасности, которая на практике реализуется в виде начальника службы безопасности (здесь сказался прошлый опыт деятельности в правоохранительных органах персонала

службы безопасности). Совершенно очевидно, что если персонал службы безопасности по количеству большой, неизбежно встает вопрос о заместителях начальника службы безопасности. Их может быть несколько (обычно по количеству подразделений службы безопасности).

Как правило, заместитель начальника службы безопасности является одновременно руководителем одного из подразделении и, в свою очередь, также имеет одного или нескольких заместителей. Не вызывает сомнений целесообразность создания таких подразделений, как канцелярия и бухгалтерия (в случае, если службу безопасности не обслуживает единая бухгалтерия предприятия-учредителя).

В крупных службах безопасности, где возникает необходимость создания штабных подразделений, так как начальники службы безопасности просто физически не способны на должном уровне выполнять такие управленческие функции, как анализ, планирование, контроль и т.д., исполнение этих обязанностей помощниками положение дел не меняет, так как в этом случае возникает необходимость их повседневного руководства, что опять-таки не под силу начальнику службы безопасности, и он вынужден будет назначить одного из них координатором деятельности других, а это, по сути, означает выполнение обязанностей начальника штаба.

Предложенная схема оргструктуры может время от времени уточняться и пересматриваться.

Любая оргструктура, даже самая оптимальная, не сможет дать ожидаемых результатов, если ее не дополнить внутренними нормативными актами, регулирующими деятельность всех подразделений и сотрудников службы безопасности. Образно выражаясь, «кость» (оргструктура) должна обрасти «мясом» (нормативными документами). Причем эти нормативные акты условно можно разделить на две группы: непосредственно относящиеся к деятельности самой службы безопасности и к деятельности других служб (подразделений, сотрудников) предприятия [7].

Методы управления службой безопасности подразделяются на три группы:

1) экономические;
2) организационно-распорядительные;
3) социально-психологические.

Руководители службы безопасности должны безупречно владеть всеми методами управления в их единстве. Для этого они должны знать особенности каждого из них. Экономические методы управления строятся на использовании различных экономических стимулов, таких, например, как заработная плата. Умелое использование этого стимула с учетом уровня профессионализма, стажа работы, результатов деятельности сотрудника и т.д. позволяет эффективно организовать работу отдельных сотрудников в рамках службы безопасности.

Организационно-распорядительные методы управления (приказы, распоряжения, указания, инструкции и т.д.) подразделяются на три группы: распорядительные, организационно-стабилизирующие и дисциплинирующие. Особое внимание в деятельности службы безопасности следует уделить таким нормативам (производные от организационно-стабилизирующих методов) как нормативы времени выполнения той или иной деятельности, численности сотрудников того или иного подразделения и т.д. Такие нормативы обычно перенимаются из опыта работы органов внутренних дел, ФСБ и т.д., с поправкой на специфику деятельности службы безопасности предприятия, фирмы.

Социально-психологические методы основаны на использовании моральных стимулов к труду и воздействуют на личность сотрудника службы безопасности с помощью психологических приемов с целью превращения задания в осознанный долг, внутреннюю потребность человека. Это достигается посредством приемов, которые носят личностный характер (личный пример, авторитет и т.д.). На уровне коллектива службы безопасности действуют методы, включающие оценку индивидуальных качеств

сотрудников и выработку ориентиров, создающих условия для максимального проявления их профессиональных качеств.

Структура процесса управления в самом общем виде состоит из трех стадий, каждая из которых включает в себя последовательно осуществляемые этапы или операции:

I стадия. Сбор, обработка, обобщение и анализ информации

II стадия. Выработка и принятие управленческого решения.

III стадия. Организация исполнения управленческого решения.

При разработке управленческих подходов для решения конкретных вопросов по предотвращению различных угроз необходимо учитывать различные режимы функционирования СПБ.

На рис. 7.1. приведена общая схема организации работ в условиях повседневной деятельности, повышенной готовности и при чрезвычайном положении (кризисной ситуации).

7.2. Функции процессов управления СБП

При рассмотрении основных процессов управления в современной теории менеджмента выделяют 4 типовых функции:

- планирование;
- организация;
- мотивация;
- контроль;

и два связывающего их процесса: коммуникации и принятия решения, подробно рассмотренные в работе [1].

Р Е Ж И М Ы

Подпись: Рис. 7.1. Режимы функционирования СБП

Применительно к рассматриваемому объекту управления СПБ, по мнению В.П. Мак-Мака [7], целесообразно выделять шесть функций:

- Прогнозирование.
- Планирование.
- Организация.
- Регулирование.
- Мотивация.
- Контроль.

В системе управления все эти функции должны быть объединены в целостный процесс, хотя из методических соображений целесообразно рассматривать их отдельно. Рассмотрим далее указанные функции с учетом специфики деятельности службы безопасности.

Прогнозирование предполагает составление заключения (прогноза) о будущих событиях и тенденциях развития службы безопасности. Прогнозные оценки бывают оперативными (с упреждением не более одного месяца), краткосрочными (от 1 месяца до 1 года), среднесрочными (от 1 года до 5 лет). Составляются они как привлеченными со стороны специалистами, так и сотрудниками службы безопасности (в первую очередь сотрудниками штаба).

Качество прогнозных оценок повышается, если они составляются сотрудниками службы безопасности с помощью приглашенных экспертов-специалистов в той или иной

области. Представляется, что наиболее целесообразным было бы составление следующих видов прогнозных оценок:

• криминологических;

• рисковых (коммерческий, финансовый и т.д.) в предпринимательской деятельности;

• экономических, физических, информационных и т.д., определяющих безопасность предприятия.

Так, в работе [7] описан набор признаков, свидетельствующих о возможных условиях для реализации преступного замысла в отношении охраняемого объекта:

1. Выявление на объекте или на прилегающей территории тайников, приспособленных преступниками для сохранения похищенного; приспособлений, с помощью которых можно проникнуть на объект; смесей, отбивающих у собаки желание работать и т.д.

2. Обнаружение охраной или сотрудниками объекта подготовленных, но замаскированных мест возможного проникновения на объект, например в районе прохождения коммуникаций через капитальные перекрытия и стены, возле длительное время неиспользуемых «черных» ходов и запасных выходов с объекта.

3. Обнаружение оторванных и приставленных к забору досок, выпиленных или выдолбленных камней, кирпичей или плит в ограждении или стене объекта.

4. Информация о случаях кражи с объектов дефицитного портативного газосварочного оборудования, а также установленные службой безопасности факты приобретения такого рода оборудования лицами с сомнительным прошлым, ранее судимыми, теми, о ком имеется информация, подтверждающая их связь с преступным миром.

5. Информация об участившихся встречах криминальных элементов с бывшими сотрудниками фирмы или ее охраны.

6. Факты краж или нападений преступников на конструктивно схожие объекты, но не охраняемые.

7. Факты угроз в адрес собственника объекта, которые могут быть как бы последней попыткой склонения фирмы (ее руководителя) к выплате определенного процента от прибыли преступникам.

8. Фиксируемые охраной факты появления возле объекта лиц, действия которых напоминают тренировочные занятия по ознакомлению с местностью, проникновению на объект или по обработке иных специальных навыков и приемов.

9. Случаи «хулиганского» разбивания стекол на объекте, стуков в двери и окна, телефонные звонки от имени людей, «ошибшихся» номером.

10. Участившиеся случаи задержания посторонних на территории объекта, а также попытки неизвестных лиц проникнуть на территорию объекта без определенных намерений.

11. Обнаружение охраной внутри объекта переброшенных снаружи мотков проволоки, досок, крупных камней, которые могут использоваться преступниками для провоцирования срабатывания сигнализации и отвлечения охраны.

12. Случаи возникновения драк и хулиганских проявлений возле объекта, повреждение автомашины сотрудников охраны, факты неожиданного отключения света на объекте.

13. Попытки криминальных элементов устроиться на работу в фирму.

14. Возникновение повышенного интереса и внимания к фирме со стороны коммерческих структур непосредственно перед прибытием на объект ценных грузов (если это обстоятельство ранее не рекламировалось).

15. Признаки возможной связи сотрудников фирмы с криминальными элементами.

Планирование предполагает определение целей, задач службы безопасности на предстоящий период деятельности, средств и времени на их достижение. Наиболее распространенными в деятельности служб безопасности являются комплексные и специальные планы.

Комплексные планы охватывают все сферы деятельности службы безопасности и включают в себя, как правило, такие разделы, как организационные вопросы обеспечения всех видов безопасности предприятия (в рамках компетенции службы безопасности), работу с кадрами, ресурсное обеспечение, контроль и т.д. Наиболее приемлемая форма составления такого плана имеет следующий вид:

№ п/п
Содержание планируемого мероприятия
Срок исп.
Ответств. за исп.
Форма представления результатов выполненного мероприятия
Отметка об исполнении
I
II
III
IV
V
VI

Существуют и другие подходы к формированию комплексных планов. Так, в работе [7] предлагается следующая структура основных разделов плана организации системы безопасности и защиты предприятия:

1. Задачи службы безопасности.

2. Выводы и оценки обстановки:

а) положение на рынке услуг (производство);

б) основные группировки сил конкурентов, преступных элементов (их построение, способы действий, возможности);

в) основные угрозы предприятию;

г) силы СБП, ее состав, возможности:

д) особенности ситуации в стране, городе (месте дислокации фирмы) и ее влияние на рынок услуг и производства.

3. Задачи, решаемые службами безопасности соседних предприятий в интересах предприятия.

4. Задачи, решаемые силами и средствами МВД в интересах предприятия.

5. Указания по взаимодействию с МВД и другими службами безопасности.

6. Организация развертывания и усиления сил СБП, техническое и материальное обеспечение их деятельности.

7. Указание (план) по организации управления силами СБП в экстремальных ситуациях (по вариантам).

8. Срок готовности сил к выполнению функциональных обязанностей в полном объеме.

Не отрицая возможности такой структуры плана, отметим, что его реализация требует согласования с органами внутренних дел и службами безопасности соседних предприятий, что в современных условиях маловероятно.

Специальные планы разрабатываются на случай возникновения чрезвычайных происшествий и чрезвычайных ситуаций (нападения на объект, угроза взрыва бомбы, захват заложников, наводнение, пожар и т.д.).

Организация – как функция состоит в установлении постоянных и временных взаимоотношений между всеми подразделениями службы безопасности, определение порядка и условий ее функционирования. Это процесс включает в себя следующие элементы:

1. Определение рациональных форм разделения труда. В сфере управления существует следующее технологическое разделение труда: технические исполнители (секретари, машинистки, операторы ЭВМ), специалисты (юристы, аналитики и т.д.) и руководители службы безопасности и его подразделений.

2.Распределение работ среди работников, групп работников. В первую очередь, такое обязательное распределение происходит между такими группами работников, как детективы и охранники (в рамках соответствующих подразделений). Во вторую очередь, работа распределяется между отделениями, секторами и группами, являющимися структурными единицами подразделений (отделов) службы безопасности. И лишь в третью очередь, работа распределяется между самими работниками. Материальное выражение такого распределения работ находит в разработке положений о подразделениях, его структурных единицах и должностных инструкциях.

3. Разработка структуры органов управления. В службе безопасности орган управления состоит из трех уровней. Высший уровень представлен начальником службы безопасности и его заместителем. Эта группа управленческих работников обеспечивает интересы и потребности руководителей предприятия-учредителя, вырабатывает политику службы безопасности и способствует ее практической реализации. Руководители среднего уровня управления (начальники подразделений) обеспечивают реализацию политики функционирования службы безопасности, разработанной высшим руководством, и отвечают за доведение более детальных заданий до своих подчиненных, а также за их выполнение. Низший уровень управления представлен младшими руководителями (начальниками отделений, групп, секторов), которые отвечают за доведение конкретных заданий до непосредственных исполнителей, а также за их выполнение.

4.Регламентация функций, подфункций, работ, операций. Такую регламентацию следует проводить, начиная последовательно с функций и заканчивая операциями. Отражать их необходимо в уставе, положениях об отделах, отделениях, группах и секторах (функции), должностных и служебных инструкциях (работы, операции). При этом очень важно обеспечить эту регламентацию таким образом, чтобы соблюдалась определенная соподчиненность между функциями, подфункциями, работами и операциями.

5. Установление прав и обязанностей органов управления и их сотрудников. Правами и обязанностями наделяются как структурные подразделения службы безопасности, так и её сотрудники. При этом важно таким образом установить обязанности, чтобы для их реализации были предоставлены соответствующие права (совпадение объема прав и обязанностей). Отражаются права и обязанности в уставе службы безопасности, положениях и должностных инструкциях. Следует при этом избегать отождествления прав и обязанностей сотрудников с правами и обязанностями службы безопасности и подразделений.

6. Подбор и расстановка кадров. Подбор кандидатов для работы в службе безопасности происходит в соответствии с требованиями, предусмотренными в законе «О частной детективной и охранной деятельности в Российской Федерации». Но в отличие от процедуры подбора кадров, где практически все вопросы жестко регламентированы, руководителям службы безопасности предоставлены определенные возможности в расстановке кадров. Такая расстановка возможна как по горизонтали, так и по вертикали.

Регулирование представляет собой «наладку» системы, приведение ее в нормальное рабочее состояние и необходимость в ней возникает в силу изменения внешних условий либо из-за возникновения каких-то нарушений, «сбоев» в функционировании самой системы. Посредством этой функции достигается поддержание

управляемых процессов в рамках, заданных программой, регламентом, планом. Орган управления службы безопасности через эту функцию должен обеспечить сохранение заданных параметров следующими приемами:

А. Выравнивание отклонений. Так, если в сравнении с аналогичным периодом прошлого года резко возросло количество краж с охраняемого объекта, то проводится комплекс мероприятий по значительному их снижению (профилактические беседы, рейды, операции и т.д.). В результате применения этого приема управляемая подсистема приводится к некой норме, удовлетворяющей руководство службы безопасности и предприятия-учредителя.

Б. Компенсация возмущений. Возмущающее воздействие внешней среды на деятельность сотрудников службы безопасности выражается иногда в отрицательном воздействии на их поведение. Такое воздействие может выражаться, например, в отказе руководства повысить им зарплату в условиях высокой инфляции, резком увеличении нагрузки и т.д. В таком случае необходимо включить так называемые компенсаторные механизмы, к примеру предоставить сотрудникам ряд материальных льгот (бесплатные питание и проезд в общественном транспорте и т.д.), увеличить количество отгулов и т.д. Реакция на возмущающее воздействие должна быть своевременной и эффективной.

В. Устранение воздействия помех. Помехи в деятельности службы безопасности могут быть как естественные (землетрясения, наводнения и т.д.), так искусственные (нападения на охраняемый объект, дискредитация руководства предприятия в средствах массовой информации, поджоги помещений и т.д.). Необходимо предварительно составить перечень (каталог) таких возможных помех и отработать систему.

Мотивация – это процесс побуждения сотрудников службы безопасности к деятельности для достижения целей самой службы и ее подразделений. Мотивация представляет собой совокупность сил, побуждающих сотрудника осуществлять деятельность с затратой определенных усилий, на определенном уровне старания и добросовестности, с определенной степенью настойчивости в направлении достижения определенных целей.

В основе любой теории мотивации лежат потребности человека, которые можно удовлетворить вознаграждениями. Причем выделяют внешние вознаграждения (заработная плата, премии и т.д.) и внутренние – чувство успеха при достижении цели, получаемое от самой работы.

Для практических целей достаточна типология с использованием трех типов мотивации: I тип - сотрудники, ориентированные преимущественно на содержательность и общественную значимость труда; II тип - преимущественно ориентированные на оплату труда и другие нетрудовые ценности; III тип - сотрудники, у которых значимость разных ценностей сбалансирована.

Среди потребностей, которые обладают конкретными мотивационно-трудовыми значениями, можно выделить следующие:

• потребность в самоуважении (добросовестная трудовая деятельность независимо от контроля и оплаты труда ради положительного собственного мнения о себе как о человеке и работнике);

• потребность в самоутверждении (высокие количественные и качественные показатели в труде ради одобрения и авторитета, похвалы, положительное отношение со стороны коллектива и руководства);

• потребность в признании (направленность трудового поведения на доказательство своей профессиональной пригодности и способностей);

• потребность в самовыражении (высокие показатели в работе основе творческого отношения к ней);

• потребность в активности (трудовая деятельность как самоцель, стремление к поддержанию через активность здоровья и самочувствия целостности личности);

• потребность в стабильности (восприятие работы как способа поддержания существующего образа жизни, достигнутого достатка);

• потребность в общении (установка на трудовую деятельность вообще и частные фрагменты работы как условия и повод для человеческих контактов и знакомств; хорошая работа как основа и тема общения).

Перечисленные моральные потребности как мотивы к труду не могут заменить собой материальные планы и ожидания. Вот почему руководители службы безопасности должны использовать в своей деятельности все формы материального и морального стимулирования своих подчиненных, добиваясь высокой мотивации их труда.

Контроль состоит в процессе соизмерения (сопоставления) фактически достигнутых результатов с запланированными. Эффективная система контроля должна соответствовать следующим требованиям:

а) контроль должен быть всеобъемлющим;

б) контроль следует сосредоточить на результате;

в) система контроля должна быть простой;

г) контроль не может быть ни целенаправленным, ни нейтральным;

д) контроль должен быть постоянным.

Субъектами контрольной деятельности в службе безопасности являются руководитель предприятия-учредителя, члены совета (комитета) безопасности предприятия, руководители службы безопасности и его подразделений (в рамках своей компетенции). Кроме этого, внешними субъектами контроля могут быть сотрудники лицензионно-разрешительных подразделений органов внутренних дел и прокуратуры.

Подконтрольными объектами могут быть деятельность подразделений, состояние технической укрепленности охраняемого объекта, защищенность коммерческой тайны, система профессиональной подготовки и переподготовки сотрудников службы безопасности и т.д. Выбор объекта контроля определяется его способностью влиять (положительно или отрицательно) на деятельность службы безопасности в целом. В рамках подконтрольного объекта очень важны его составные элементы, после определения которых можно непосредственно приступить к контролю. Так, в рамках проверки состояния защиты коммерческой тайны на предприятии должны быть изучены:

1) соблюдение норм, правил хранения и охраны в помещениях, спецхранилищах, на рабочих местах носителей информации;

2) ведение учета и обеспечение личной ответственности за выполнение данной функции;

3) соблюдение порядка хранения и уничтожения засекреченных сведений;

4) соблюдение требований порядка обращения с носителями коммерческой тайны;

5) меры по предотвращению несанкционированного выноса носителей коммерческой тайны за территорию предприятия.

7.3. Принципы управления СБП

Принципы управления службой безопасности определяют требования к системе структуре и организации процесса управления. В рамках службы безопасности это следующие принципы [7]:

1. Научность. Основное содержание этого принципа заключается в требовании, чтобы все управленческие действия осуществлялись на базе применения научных методов и подходов. Между прочим, этот принцип требует от руководителей службы безопасности и его подразделений внимательного изучения управленческой и специальной литературы по проблемам обеспечения безопасности предприятия.

2. Единоналичие и коллегиальность. Сущность этого принципа заключается в том, что на основе мнений низовых руководителей и рядовых исполнителей конкретных решений, вышестоящий начальник пользуется правом единоличного решения вопросов, входящих в его компетенцию.

3. Принцип системности и комплексности. Системность означает необходимость использования элементов теории больших систем, системного анализа в каждом управленческом решении. Комплексность в управлении означает необходимость всестороннего охвата управляемой системы, учета всех сторон, всех направлений, всех свойств. Этот принцип требует от руководителей службы безопасности выработки у себя аналитико-синтетического склада мышления.

4. Принцип системности и комплексности. Этот принцип состоит в оптимальном распределении (делегировании) полномочий при принятии управленческих решений. Здесь следует руководствоваться таким правилом: тот, кому предстоит выполнять управленческое решение, должен его самостоятельно разработать и, с учетом возможных корректив вышестоящего руководства, активно добиваться его реализации.

5. Принцип плановости. Сущность этого принципа состоит в установлении основных направлений и пропорций службы безопасности в перспективе. Практическая реализация этого принципа означает, что все сотрудники, подразделения и службы безопасности в целом должны планировать свою деятельность в такой последовательности: служба безопасности - подразделения - сотрудник.

6. Принцип сочетания прав, обязанностей и ответственности. Этот принцип предполагает, что каждый сотрудник службы безопасности должен выполнять возложенные на него обязанности, при этом он наделяется адекватными ему правами и несет ответственность за качество их выполнения.

7.4. Обеспечение деятельности службы безопасности

Для успешного функционирования и эффективного управления службой безопасности необходимо обеспечить ее материально-техническими, финансовыми, кадровыми и информационными ресурсами [11].

Среди них первостепенное значение имеют финансовые ресурсы. Без финансового обеспечения деятельности службы безопасности бессмысленно вообще говорить о ее функционировании.

Поскольку служба безопасности не вправе самостоятельно зарабатывать деньги путем заключения договоров с другими клиентами, именно на предприятии-учредителе лежит обязанность финансирования ее деятельности. Но это не означает, что руководство службы безопасности должно занимать в этом вопросе пассивную позицию. Напротив, обоснованные текущие и прогнозные оценки в финансовых потребностях службы безопасности и основанные на них точные расчеты должны стать правилом, а не исключением. Финансовую политику службы безопасности определяют, конечно, ее руководители, но при этом активную помощь им должна оказывать бухгалтерская служба.

В функции этой службы входит ведение табеля, учета рабочего времени; начисление зарплаты, премий и т.д.; учет выплат за различные услуги; перечисление денег; выдача сотрудникам их денежного содержания; оплата счетов и т.д. Поскольку руководители службы безопасности не являются, как правило, специалистами в финансовых вопросах, наиболее целесообразно свое внимание сосредоточить им на некоторых ключевых моментах.

Во-первых, периодически проверять финансовое состояние службы безопасности с помощью приглашенных специалистов. Во-вторых, открывать расчетные и текущие счета только в надежных банках. В-третьих, добиваться такого уровня минимальной зарплаты персонала службы безопасности, чтобы у него не возникало соблазна увольняться (можно порекомендовать в связи с этим устанавливать в контрактах сумму зарплаты в

иностранной валюте по курсу Центрального банка России на день его выдачи). В-четвертых, установить поэтапное финансирование закупленных (приобретенных) материально-технических средств от наиболее необходимых (например, в первую очередь, оружие, спецсредства) до менее необходимых (например, канцелярские принадлежности и т.д.). Наконец, рационально и обоснованно использовать деньги из фонда поощрения и материальной помощи персоналу [7].

Полное и качественное обеспечение деятельности службы безопасности материально-техническими ресурсами - не только средство, но и условие повышения эффективности работы его сотрудников Эти ресурсы условно подразделяются на следующие группы:

• оружие и боеприпасы;

• специальные средства;

• служебные помещения различного характера (кабинеты, караульные помещения, оружейные комнаты, стрелковые тиры, комнаты досмотра);

• вспомогательная техника (автотранспорт, видео, -кино, -фототехника, средства оперативной радио- и телефонной связи, компьютеры и т.д.);

• средства предупреждения и защиты (охранно-пожарная сигнализация, сторожевые собаки, охранное освещение, телевидение т.д.);

• средства обеспечения нормальной деятельности сотрудников (форменное обмундирование, мебель, канцелярские принадлежности, медикаменты, бланки документов, юридическая и специальная литература и т.д.).

Обеспечение оружием, боеприпасами, спецсредствами сотрудников службы безопасности регламентировано законом и нормативными актами правительства, МВД и Министерства финансов России. В отношении обеспечения некоторых средств целесообразно использовать нормативы, имеющиеся в различных министерствах и ведомствах (количество служебных собак, оборудование и размеры стрелкового тира, наличие медикаментов, расчет различных видов охранно-пожарной сигнализации и т.д.).

Наконец, последнее по счету, но не по важности, обеспечение деятельности службы безопасности информационными ресурсами.

Прежде всего, следует определить потребность и объемы минимума информации, без которых функционирование службы безопасности вообще невозможно. Такую информацию можно условно разделить на три блока («Среда функционирования предприятия», «Состояние безопасности внутри предприятия» и «Внутриорганизационная деятельность службы безопасности»), после чего в рамках каждого блока разработать перечень необходимых сведений. Этот перечень не будет носить произвольный характер, если при его составлении руководствоваться одним принципом: любая информация реально должна «обслуживать», «работать» на реализацию, как минимум, одной функции службы безопасности. Можно рекомендовать в этой связи включать в указанные блоки следующие сведения, которые, разумеется, не могут быть исчерпывающими [7].

В 1-й блок «Среда функционирования предприятия» возможно включение сведений о предприятиях-конкурентах, правоохранительных и контрольно-надзорных органах, рыночной конъюнктуре, криминогенной ситуации в районе месторасположения предприятия, нормативных актах, регулирующих деятельность предприятия-учредителя и т.д.

Во 2-й блок «Состояние безопасности внутри предприятия» целесообразно включить следующие сведения: состояние преступности среди персонала, наличие или отсутствие коммерческой тайны, источники (каналы) и суммы материального ущерба, наносимого предприятию, анализ насильственных преступлений, совершенных против его персонала, эффективность работы юрисконсульта (юридической службы), о сотрудниках предприятия, имеющих доступ к конфиденциальной информации, с корыстно-насильственной мотивацией, связанных с сохранностью товарно-материальных ценностей; местонахождении и правилах работы с документацией, содержащей

коммерческую тайну; месторасположении и состоянии сохранности изделий (описания процесса), составляющих секрет предприятия и т.д.

Наконец, в 3-м блоке «Внутриорганизационная деятельность службы безопасности» желательно иметь сведения о составе и структуре службы безопасности, перемещениях сотрудников, дисциплинарной практике, результатах проверок, состоянии законности и т.д.

Совершенно очевидно, что без надлежащей организации такого массива информации, удобной и практичной для использования, не обойтись. Идеальным вариантом в этом случае было бы создание информационной системы на базе компьютерной техники, однако его создание требует определенных финансовых затрат. Поэтому на практике чаще всего встречается отражение и систематизация необходимой информации в письменных документах. К документам, составляемым в службе безопасности, относятся:

. организационные документы (устав, положение, должностные инструкции, штатное расписание, правила внутреннего трудового распорядка);

. правовые документы (законы, подзаконные акты, методические рекомендации по проблемам безопасности и т.д.);

. распорядительные документы (приказы, инструкции, указания, графики работы персонала и т.д.);

. информационно-справочные документы (протоколы, акты, справки, письма, докладные и объяснительные записки, телефонограммы, телеграммы, досье и т.д.);

. договоры, трудовые соглашения;

. документы по личному составу (приказы по личному составу, трудовые книжки, материалы проверок по жалобам, графики отпусков и т.д.).

В результате правильно организованного документального отражения необходимых сведений достигается эффективное информационное обеспечение деятельности службы безопасности.

Не менее важное значение для руководителей службы безопасности имеет вопрос кадрового обеспечения ее деятельности. Работу эту условно можно разделить на два этапа.

На первом этапе происходит отбор кандидатов для работы в службе безопасности, их проверка, прохождение ими специальной подготовки и стажировка в должности. При отборе кандидатов особое внимание должно уделяться их образованию (помимо юристов, целесообразно приглашать на работу экономистов, финансистов и в последнее время специалистов по защите информации). Помимо проверки через органы внутренних дел, проводится дополнительное выяснение биографических и других характеризующих личность кандидата данных. Разумеется, это необходимо делать не во всех случаях (излишней будет такая проверка, например, кандидата, которого хорошо и давно знает руководитель службы безопасности) и с письменного согласия кандидатов. Однако письменное согласие на проверку такого рода после зачисления кандидата в службе безопасности необходимо получать в любом случае.

Если в процессе проверки установлена пригодность кандидата для работы в службе безопасности, то его направляют на учебу в негосударственное образовательное учреждение (за исключением лиц, имеющих стаж работы в оперативных или следственных подразделениях не менее трех лет). При этом особое внимание обращается на наличие лицензии у этого учреждения и качество программы обучения. После прохождения специальной подготовки и получения лицензии охранника или детектива целесообразно организовать стажировку его в соответствующей должности (от 1 до 6 мес.) и лишь после этого решать вопрос об его зачислении на постоянную работу в службе безопасности или увольнении. Разумеется, такая возможность должна быть предусмотрена в контракте, который подписывается после отбора кандидата.

7.5. Управление безопасностью предприятия в кризисных ситуациях

Служба безопасности должна быть всегда готова к возникновению критических (кризисных) ситуаций, проявляющихся в результате столкновения интересов бизнеса и преступного мира.

Кризисная ситуация – это проявление фактов угроз со стороны отдельных лиц или групп. Кризисная ситуация может проявляться и развиваться по-разному: медленно или спонтанно, мгновенно [13].

При оценке и анализе кризисной ситуации очень важно как можно быстрее определиться с ответом на вопрос, способна ли СБП справиться с ситуацией своими силами либо для ее разрешения необходимо привлечение правоохранительных органов. Однако в любом случае, учитывая возможность возникновения кризисных ситуаций, любая фирма стремится создать в составе СБП отдельное формирование, именуемое КРИЗИСНАЯ ГРУППА. Она создается из числа ключевых фигур фирмы: директор, руководители линейных подразделений, филиалов, служб, юрист, главный бухгалтер и др. Кризисная группа может быть создана на постоянной основе с непременным включением в число ее членов:

- руководителя фирмы;
- юриста;
- финансиста;
- руководителя службы безопасности.

Руководство кризисной группой может быть возложено на главу фирмы. Перечисленные лица, как правило, в силу своего служебного положения, обладания специальными знаниями, опытом располагают реальными возможностями достаточно эффективно воздействовать на обстоятельства, в условиях которых возникает и протекает кризисная ситуация, не выпуская при этом рычагов влияния на повседневную коммерческую и производственную деятельность.

В каждом конкретном случае в состав кризисной группы могут включаться и иные специалисты.

Кризисная группа решает следующие задачи:

. оценка обстановки;

. принятие неотложных мер по безопасности;

. управление деятельностью фирмы в экстренных условиях;

. обеспечение оперативного взаимодействия с органами правопорядка.

Главная цель создания кризисной группы – противодействие внешним угрозам безопасности фирмы. Рабочие заседания группы должны проходить в условиях предельной конфиденциальности. Как правило, деятельность кризисной группы регламентируется типовым планом действий руководства и персонала фирмы. В зависимости от складывающейся ситуации планы могут быть следующего вида, а именно, план действий:

. при угрозе взрыва;

. захвате заложников или похищении сотрудников фирмы;

. вымогательстве;

. нападении на помещения фирмы;

. нападении на инкассаторов.

Типовые кризисные планы являются документами конфиденциального характера, доступ к которым должен иметь узкий круг лиц. Составляться подобные планы должны не более чем в двух-трех экземплярах. Один хранится у руководителя, другой – у

начальника службы безопасности, третий может находиться у лица, замещающего руководителя фирмы в его отсутствие.

Осуществляя планирование, надо исходить из того, что план – это не набор мероприятий, а последовательная линия поведения, стратегия деятельности фирмы в конкретной кризисной ситуации, направленная на обеспечение эффективной безопасности.

Контрольные вопросы

1. Назовите три группы методов управления службой безопасности.
2. Какие функции рассматриваются при управлении СБП?
3. В чем выражается прогнозирование ситуации со стороны сотрудников СБП?
4. Какие разделы включают в план при организации системы безопасности?
5. Что включает в себя функция «организации» при управлении СБП?
6. Перечислите основные потребности сотрудников, используемые для их мотивации в условиях управления СБП.
7. Кто и кого должен контролировать при управлении СБП?
8. Перечислите принципы управления СБП.
9. Назовите четыре вида обеспечения деятельности СБП.
10. Чем отличается управление СБП в крупной ситуации от обычного режима работы?

Глава 8. Подбор, расстановка и обучение сотрудников службы защиты информации

8.1. Роль персонала в системе защиты информации

Системы защиты и охраны проектируют, строят и используют люди, обслуживают технику и технологический процесс любого предприятия также люди. Они должны быть надежны: честны, внимательны, аккуратны и исполнительны. Самая высокая задача в охране и защите информации предприятия – обеспечение надежности обслуживающего персонала.

Обеспечение надежности персонала службы защиты информации - это совокупность мер, включающих в себя анализ и оценку степени честности и благонадежности сотрудников с целью гарантировать защиту информации, обеспечить ее целостность и конфиденциальность.

К мерам по обеспечению надежности персонала относятся:

• выполнение обязательств сотрудниками в том, что они будут обеспечивать защиту и тайну информации, к которой они имеют доступ в силу своих профессиональных обязанностей;

• создание благоприятного производственного климата для всех сотрудников службы безопасности.

Согласно существующей статистике, в коллективах людей, занятых той или иной деятельностью, как правило, только около 85% являются вполне лояльными, а остальные 15% делятся примерно так: 5% – могут совершить что-нибудь противоправное, если, по их представлениям, вероятность заслуженного наказания мала; 5% - готовы рискнуть на противоправные действия, даже если шансы быть уличенным и наказанным складываются 50 на 50%; 5% – готовы пойти на противозаконный поступок, даже если они почти уверены в том, что будут уличены и наказаны. Такая статистика в той или иной мере может быть применима к коллективам, участвующим в разработке и эксплуатации информационно-технических составляющих компьютерных систем. Таким образом, можно предположить, что не менее 5% персонала, участвующего в разработке и эксплуатации программных комплексов, способны осуществить действия криминального характера из корыстных побуждений либо под влиянием каких-нибудь иных обстоятельств.

Имеющийся зарубежный и отечественный опыт защиты производственных и коммерческих секретов свидетельствует, что без активного вовлечения в этот процесс всех сотрудников, имеющих доступ к конфиденциальной информации, результат не может быть полным. Специалисты по защите информации приводят данные, утверждающие, что определяющей фигурой в обеспечении сохранности ценных сведений предприятия является его сотрудник. Анализ угроз информации позволил выделить следующие виды угроз информационным ресурсам – по возрастанию степени их опасности:

1) некомпетентные служащие;
2) хакеры и крекеры;
3) неудовлетворенные своим статусом служащие;
4) нечестные служащие;
5) инициативный шпионаж;
6) организованная преступность;
7) политические диссиденты;
8) террористические группы.

Угроза, исходящая от некомпетентности служащих, по мнению экспертов, основывается на алгоритмической уязвимости информационных систем, которая не исключает возможности некомпетентных действий и может привести к сбоям системы. Неудовлетворенные служащие также предоставляют внутреннюю угрозу. Они опасны тем, что имеют легальный доступ. То же можно сказать и про нечестных служащих.

В связи с этим представляется целесообразным с целью обеспечения информационной безопасности коммерческих структур уделять большее внимание подбору и изучению кадров, проверке любой информации, указывающей на их сомнительное поведение и компрометирующие связи.

Следует особо подчеркнуть, что наиболее неуправляемым элементом в системе защиты информации является персонал. Правильная кадровая политика и организация управления персоналом позволяют снизить риски этого фактора. Задача обеспечения информационной безопасности должна решаться на всех уровнях управления предприятием. Рассмотрим их более подробно в трех направлениях [24].

1. Безопасность при выборе персонала и работе с ним

Необходимо включить задачи по обеспечению безопасности в должностные обязанности всех сотрудников. При приеме на работу рекомендуется проводить:

• проверку рекомендаций;
• проверку данных из резюме;
• подтверждение ученых степеней и образования;

• идентификацию личности;
• проверку на полиграфе при добровольном согласии кандидата на должность;
• включение соглашения о соблюдении режима информационной безопасности в условия трудового договора с работником.

При приеме на работу новых сотрудников необходимо, чтобы они ознакомились и подписали:
. письменную формулировку:
• их должностных обязанностей;
• прав доступа к ресурсам компании (в том числе и информационным);
. соглашение о конфиденциальности;
. специальные соглашения об ознакомлении со всеми видами служебной корреспонденции (мониторинг сетевых данных, телефонных переговоров, факсов и т.д.).

2. Подготовка и переподготовка пользователей и специалистов по защите информации.
Необходимо иметь систему повышения уровня технической грамотности и информированности пользователей в области информационной безопасности, а также переподготовки специалистов по защите информации. Для этого необходимы регулярное проведение тренингов для персонала и контроль готовности новых сотрудников по применению правил информационной защиты, а также периодическая переподготовка специалистов подразделений защиты информации. Особенно важно проводить тренинги при изменении конфигурации информационной системы (внедрении новых технологий и прикладных автоматизированных систем, смены оборудования, операционной системы, ключевых приложений, принятии новых правил или инструкций и т.д.)

3. Реагирование на нарушения информационной безопасности.
Для организации своевременного реагирования на нарушения информационной безопасности необходимо создать систему аудита событий информационной безопасности, которая должна включать средства системного анализа для автоматизированных участков обработки информации, а также регламент представления отчетов об инцидентах в области информационной безопасности для всех сотрудников предприятия и другую информацию о состоянии системы защиты, а именно: отчеты . об инцидентах; . недостатках в системе безопасности; . сбоях и неисправностях компьютерных систем.

Регламент реагирования на нарушения информационной безопасности или в случае обнаружения нестандартной ситуации должен предусматривать:
• регистрацию всех симптомов проявления нарушения;
• изоляцию компьютера и, если возможно, приостановку его использования;
• немедленный отчет о факте нарушения непосредственному руководителю и службе информационной безопасности;
• запрет на принятие самостоятельных действий, не регламентированных документами или несанкционированными службой защиты информации;
• изучение инцидента, отчет о результатах анализа причин произошедшего;
• дисциплинарные, административные или уголовные меры воздействия на нарушителей.

8.2. Набор и отбор персонала в СБП

Набор и отбор кадров – одно из самых важных направлений деятельности отдела управления персоналом, так как от квалификации, заинтересованности и надежности

работников напрямую зависит будущее компании. Набором служащих для производства и кадров для службы безопасности занимается отдел управления персоналом, а руководство СБП осуществляет тщательный контроль за этим процессом. Но перед тем, как проводить непосредственный набор, надо оценить имеющиеся ресурсы и сделать прогноз численности персонала, необходимого для реализации краткосрочных и перспективных целей, а затем, определив будущие потребности, руководство должно разработать программу их удовлетворения [25].

Для того, чтобы выбрать наиболее подходящего работника для данной должности, необходимо провести анализ рабочего места. Основная цель этого – выявить, каким психологическим требованиям должен соответствовать кандидат, и составить портрет идеального сотрудника, характеристики которого полностью соответствуют требованиям рабочего места, и отобрать такого претендента, который будет трудиться с максимальной отдачей и чувствовать себя комфортно на данной работе.

Объем работ на этом этапе определяется разницей между имеющимися кадрами и настоящей или будущей потребностью в них. При этом необходимо учитывать такие факторы, как выход на пенсию, текучесть кадров, увольнения в связи с истечением срока трудового соглашения о найме, расширение сферы деятельности организации. Набор обычно ведется из внешних и внутренних источников рабочей силы.

Для проведения набора могут быть использованы известные методы, применяемые в менеджменте персонала:

1 .Поиск внутри организации. Прежде чем выйти на рынок труда большинство организаций пробуют искать кандидатов в «собственном доме». Наиболее распространенными методами внутреннего поиска являются объявления о вакантном месте во внутренних средствах информации: газетах предприятия, стенных газетах, специально изданных информационных листках, а также обращение к руководителям подразделений с просьбой выдвинуть кандидатов и анализ личных дел с целью подбора сотрудников с требуемыми характеристиками. Поиск внутри организации, как правило, не требует значительных финансовых затрат, способствует укреплению авторитета руководства в глазах сотрудников. В то же время внутренний поиск часто наталкивается на сопротивление со стороны руководителей подразделений, стремящихся «скрыть» лучших сотрудников и сохранить их «для себя». Кроме того, при поиске кандидатов внутри организации возможности выбора ограничены числом ее сотрудников, среди которых может не оказаться необходимых людей.

2. Подбор с помощью сотрудников. Отдел человеческих ресурсов может обратиться к персоналу организации с просьбой оказать помощь и заняться неформальным поиском кандидатов среди своих родственников и знакомых. Этот метод привлекателен, во-первых, низкими издержками, а, во вторых, достижением довольно высокой степени совместимости кандидатов с организацией за счет их тесных контактов с представителями организации. Его недостатки связаны с «неформальностью» – рядовые сотрудники не являются профессионалами в области подбора кандидатов, не всегда владеют достаточной информацией о рабочем месте, вознаграждении и т.д., часто не объективны в отношении потенциала близких им людей.

3. Самопроявившиеся кандидаты. Практически любая организация получает письма, телефонные звонки и другие обращения от людей, занятых поисками работы. Не имея потребности в их труде в настоящий момент, организация не должна просто отказываться от их предложения – необходимо поддерживать базу данных на этих людей; их знания и квалификация могут пригодиться в дальнейшем. Поддерживание таких баз данных обходится недорого и позволяет иметь под рукой представительный резерв кандидатов.

4. 0бъявления в средствах массовой информации – на телевидении, радио, в прессе. Основное преимущество данного метода подбора кадров – широкой охват населения при относительно низких издержках. Недостатки являются обратной стороной преимуществ –

объявления в средствах массовой информации могут привести к огромному наплыву кандидатов, большинство из которых не будет обладать требуемыми характеристиками. Данный метод с успехом используется для подбора кандидатов массовых профессий, например строительных рабочих для возведения нового объекта. Для привлечения специалистов объявления помещаются в специальной литературе (финансовые или бухгалтерские издания). Такая сфокусированность поиска ограничивает число потенциальных кандидатов, обеспечивает более высокий уровень их профессионализма и значительно облегчает последующий отбор.

5.Выезд в институты и другие учебные заведения. Многие ведущие организации постоянно используют этот метод для привлечения молодых специалистов. Выезжая в учебные заведения, организация проводит презентацию компании, организуя выступления руководства, демонстрацию продукции, видеофильмов организации, отвечая на вопросы студентов и проводя собеседования с будущими выпускниками, заинтересовавшимися их организацией. Этот метод является очень результативным для привлечения определенного типа кандидатов – молодых специалистов. В то же время область применения данного метода ограничена, так как вряд ли кто-либо отправится искать генерального директора в институт.

6.Государственные агентства занятости. Правительства большинства современных государств способствуют повышению уровня занятости населения, создавая для этого специальные органы, занятые поиском работы для обратившихся за помощью граждан. В Российской Федерации такие учреждения, называемые Федеральными бюро по трудоустройству, существуют в каждом административном округе. Каждое бюро имеет базу данных. Организации, занятые поиском сотрудников, имеют доступ к этой базе данных. Использование государственных агентств дает возможность провести сфокусированный поиск кандидатов при незначительных издержках. Однако данный метод редко обеспечивает широкий охват потенциальных кандидатов.

7.Частные агентства по подбору персонала. Подбор персонала превратился за последние 30 лет в бурно развивающуюся отрасль экономики, во многих странах, в том числе и у нас, сегодня существуют сотни частных компаний, специализирующихся в этой области. Каждое агентство имеет свою базу данных, а также осуществляет специальный поиск кандидатов в соответствии с требованиями клиента. Частные агентства обеспечивают достаточно высокое качество кандидатов, их соответствие требованиям клиента и, тем самым, значительно облегчают дальнейший процесс отбора. Высокие издержки являются фактором, ограничивающим широкое применение данного метода, который используется в случаях поиска руководителей и специалистов, оказывающих значительное влияние на функционирование организации.

Анализ представленных методов подбора кандидатов позволяет сделать простой, но исключительно важный вывод – не существует одного оптимального метода, поэтому отдел человеческих ресурсов должен владеть всем набором приемов для привлечения кандидатов и использовать их в зависимости от конкретной задачи. Большинство специалистов сходятся во мнении, что для успешной организации поиска кандидатов следует руководствоваться двумя основными правилами:

. всегда проводить поиск кандидатов внутри организации;

. использовать, по меньшей мере, два метода привлечения кандидатов со стороны.

После анализа рабочего места и набора претендентов осуществляется отбор будущих работников. Отбор – это процесс, с помощью которого предприятие или организация выбирает из ряда заявителей одного или нескольких, наилучшим образом подходящих под критерии отбора на вакантное место. Каковы критерии отбора? Их обычно устанавливает менеджер соответствующего профиля. Так, в качестве общих критериев, предъявляемых к сотрудникам СБП, можно выделить следующие:

. образование (не ниже среднего);

. специальная подготовка;

. коммуникативность, активность, умение строить отношения с людьми;

. психологическая уравновешенность;

. умение принимать решения в экстремальных ситуациях;

. знание необходимых нормативных документов, регламентирующих деятельность СБП;

. знание основ уголовного права, правового-процессуального кодекса.

Для работников производства критерии отбора определяет начальник соответствующего профиля. Наиболее общими являются следующие критерии:

1. Формальное образование (при равных показателях работодатели предпочитают большее образование меньшему и большее его соответствие конкретной работе).

2. Опыт (работодатели часто отождествляют опыт с возможностями работника; одним из способов измерения опыта работы является установление рейтинга трудового стажа).

3. Физические, медицинские характеристики (для работ, требующих физической выносливости и силы).

4. Персональная характеристика, социальный статус (некоторые работодатели предпочитают «степенных», женатых работников).

5. Тип личности (работодатели могут предпочитать определенные типы личности для выполнения различных работ).

В этом отношении интересен опыт многих предприятий США [25]. В прошлом отбор персонала на них во многом считался довольно простым решением. Начальник лично беседовал с желающими и сам их распределял, руководствуясь исключительно своей интуицией. Решения принимались на основе приязней и неприязней начальника. Сегодня отбор рассматривается как нечто большее, чем вера в интуицию.

Решение при отборе обычно состоит из нескольких ступеней, которые следует пройти заявителям. На каждой ступени часть заявителей отсеивается или же они сами отказываются, принимая другие предложения. Так, широко используется следующая схема решений по отбору с прохождением определенных ступеней (естественно, число ступеней зависит от возможностей, профиля фирмы и каждой конкретной должности – здесь указан один из максимальных вариантов) [25]:

СТУПЕНЬ 1. Предварительная беседа по отбору.

СТУПЕНЬ 2. Заполнение бланка заявления.

СТУПЕНЬ 3. Беседа по найму.

СТУПЕНЬ 4. Тесты по найму.

СТУПЕНЬ 5. Проверка рекомендаций и обязательств перед другими фирмами.

СТУПЕНЬ б. Медицинский осмотр.

СТУПЕНЬ 7. Принятие решения.

Конечно, не все организации реализуют все ступени, поскольку это требует много времени и больших затрат. Однако слабая процедура отбора приведет к тому, что организация потом потратит большие средства на обучение и переобучение персонала, а также к другим негативным последствиям (в частности связанных с нарушением коммерческой тайной фирмы). В целом, чем важнее пост, тем вероятнее использование приемов каждой ступени, например для работников СБП необходимо пройти больше ступеней, чем для работников производства.

Трудно определить риск найма работника, пока не будет получена полная информация о характере тех данных, которые он использовал на предыдущей работе. Надо постараться побудить кандидата быть искренним. Если чувствуется, что он что-то недоговаривает, попробовать проверить это путем запроса рекомендаций с прежнего

места работы или воспользоваться услугами частных агентств. Эти мероприятия позволят избежать судебного разбирательства из-за разглашения чужой коммерческой тайны.

В США есть специальные организации, которые добывают рекомендации с прежнего места работы и составляют общие сведения о претенденте. Закон только требует, чтобы добываемая информация не нарушала права человека и предоставлялась только тем лицам, которые принимают решение об отборе кандидатов. Однако правила этих компаний требуют, чтобы претендент на работу был оповещен заранее о проводимом исследовании. Претендент должен быть также оповещен о причине отказа ему в должности. За ним остается право пересмотра информации, из-за которой ему отказали в назначении. Кроме того, работодатель обязан сообщить кандидату название агентства, которое добыло данную информацию.

Рекомендации при проверке и отборе кадров в службу защиты информации. С точки зрения обеспечения защиты информации являются обязательными следующие основные функции по отбору кандидатов на работу:

. определение степени вероятности формирования у кандидата преступных наклонностей при возникновении в его окружении определенных благоприятных обстоятельств;

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

Для добывания подобной информации используются возможности различных подразделений коммерческих структур, в первую очередь службы безопасности, отдела кадров, юридического отдела, подразделений медицинского обеспечения, а также некоторых сторонних организаций, например детективных агентств, бюро по занятости населения, диспансеров и пр. Для сбора сведений такого характера применяются в соответствии с законом «О частной детективной и охранной деятельности в РФ» 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.

Очевидно также, что представители служб безопасности должны быть абсолютно уверены в том, что проводят тесты, собеседования и встречи именно с теми лицами, которые выступают в качестве кандидатов на работу. Это подразумевает тщательную проверку паспортных данных, иных документов, а также получение фотографий кандидатов без очков, контактных линз, парика, макияжа. Необходимо требовать предоставления комплекта фотографий. Рекомендуется настаивать на получении набора цветных фотографий кандидата в связи с тем, что они четко и без искажений передают цвет волос, кожи, возраст и характерные приметы.

В практике уже известны случаи, когда для дополнительного анализа анкеты кандидата и его фотографий руководители служб безопасности приглашали высоко профессиональных юристов, графологов, известных психоаналитиков и даже экстрасенсов с целью обеспечения максимальной полноты формулировок окончательного заключения и выявления возможных скрытых противоречий в характере проверяемого лица. В последние годы широко практикуется почерковедческая экспертиза, которая позволяет определить многие черты характера кандидата: темперамент, выдержку, волевые качества, собранность, аккуратность, грамотность, общеобразовательный уровень и пр., а также предрасположенность к совершению неблаговидных и нечестных поступков.

В том случае, если результаты работы 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).

Особенности проверки руководящих кадров. Особое значение приобретает подбор и проверка лиц, принимаемых на ответственные вакантные должности в коммерческих структурах (члены правлений, главные бухгалтеры, консультанты, начальники служб безопасности и охраны, руководители компьютерных центров и цехов, помощники и секретари первых лиц). Сегодня кандидаты на такие должности подвергаются, как правило, следующей стандартной проверке, включающей:

. достаточно продолжительные процедуры сбора и проверки установочно-биографических сведений с их последующей аналитической обработкой;

. предоставление рекомендательных писем от известных предпринимательских структур с их последующей проверкой;

. проверки по учетам правоохранительных органов;

. установки по месту жительства и по предыдущим местам работы; серии собеседований и тестов с последующей психоаналитической обработкой результатов.

По мнению экспертов, даже каждый взятый в отдельности из упомянутых методов проверки достаточно эффективен. В совокупности же достигается весьма высокая степень достоверности информации о профессиональной пригодности и надежности кандидата, его способностях к творческой работе на конкретном участке в соответствующем коммерческом предприятии. Ниже, в качестве примера, приведены условия для приема на работу на должность начальника службы безопасности.

ТРЕБОВАНИЯ К СОИСКАТЕЛЮ ВАКАНТНОЙ ДОЛЖНОСТИ

Формальные требования:

Возраст: до 45 лет. Образование: высшее, предпочтение кандидатам силовых структур (МО, МВД, ФСБ, подразделений режимных объектов), посещение семинаров и тренингов (по актуальным вопросам обеспечения безопасности).

Наличие сертификатов на ношение оружия, осуществление охранной деятельности является для кандидата неоспоримым преимуществом. Опыт работы: от 3-х лет в организации службы, подбор персонала для службы безопасности, проверка работников предприятия на лояльность к компании, знание юридических основ охранной деятельности.

Личностные характеристики:

Хорошие организаторские навыки. Потребность в профессиональном и карьерном росте. Жёсткость в постановке задач и контроле их выполнения. Высокий уровень лояльности к компании. Наличие чётких карьерных и жизненных приоритетов.

УСЛОВИЯ НАЙМА СОТРУДНИКА:

График работы: пятидневная рабочая неделя с 8.00 до 17.00. Вознаграждения и компенсация: компания с успешными кандидатами ведет переговоры от 500 $ (оклад) + система бонусов по результатам работы компании и по личным результатам кандидата + оплата сотовой связи + ГСМ + медицинская страховка.

Испытательный срок: 3 месяца.

Работа отдела по подбору персонала, особенно если она координируется службой безопасности, позволяет в определенной степени отсеивать случайных людей. Однако оценка качеств, характеризующих степень психологической и социальной надежности кандидата или уже работающего на ключевой должности сотрудника (прежде всего здесь имеются в виду лица, допущенные к материальным ценностям и коммерческой тайне), не всегда может быть эффективно и относительно быстро произведена без специалистов и

определенного рода инструментария. При решении руководителями организации вопроса надежности персонала обычно используются два пути. Первый, и наиболее распространенный, характерен для небольших компаний: подбор сотрудников по рекомендациям друзей, знакомых или родственников. Второй путь - проведение дополнительного контроля службой безопасности предприятия (банка) или силами правоохранительных органов. Однако люди, способные совершать неблаговидные поступки в основной своей массе не являются злостными правонарушителями, то есть не состоят на учете в милиции. Что касается характеристик друзей или родственников, то их мнение далеко не всегда может быть объективным.

Таким образом, если профессиональные умения, навыки и деловая квалификация сотрудника проявляются достаточно быстро, то о действительных намерениях человека, его честности и порядочности по отношению к фирме можно судить лишь спустя некоторое время, когда предупредительные меры применять зачастую уже поздно.

Практика работы в сфере определения профессиональной психологической и социальной надежности показала целесообразность и эффективность включения в схему работы с персоналом ряда специальных мероприятий, а именно: применение глубинного психологического тестирования и специальных проверок на полиграфе.

В ходе психологического тестирования обосновываются выводы с предупреждением о наличии в психике и характере обследуемого возможных ограничений к использованию в планируемой должности.

Целью психологического тестирования является также получение и доведение до лица, принимающего решение, объективной информации об интеллектуальных способностях и мотивационно-ценностной направленности личности (прогноз лояльности).

В заключение, по первичному тестированию, дается профориентационный профиль личности кандидата, а также оценивается предрасположенность к определенного рода нежелательному для фирмы поведению. Так, методика психологического тестирования позволяет выявить предрасположенность личности к определенного рода зависимостям - наркотической, алкогольной, азартному поведению и т.п.

Обычно заказчик обследования желает получить ответ на вопросы:

. не имеет ли кандидат на вакантную должность вредных наклонностей (алкоголизм, наркомания, азартное поведение и т.п.);

. не скрывает ли сведения о совершенных в прошлом уголовно наказуемых деяниях;

. верно ли сообщил данные о прежних местах работы;

. лоялен ли по отношению к руководству фирмы и не имеет ли каких-либо связей с конкурирующими фирмами;

. имел или имеет связи с криминальным миром;

. определяются возможные варианты финансовой или другого рода зависимостей от нежелательных для фирмы лиц или организаций.

Кроме того, данное обследование имеет еще и психологически формирующее значение, так как для кандидата или сотрудника фирмы конкретно выделяются вопросы, нарушение которых влечет за собой определенного рода ответственность. Буквально, в сознании и подсознании человека формируются определенные барьеры, через которые нельзя переступать. При работе с кадрами регулярные или выборочные эпизодические обследования персонала могут быть использованы в профилактических целях, для предотвращения хищений и выявления каналов утечки конфиденциальной информации.

Применение полиграфа показало себя наиболее эффективным инструментом отбора сотрудников и проверки правдивости предоставляемых ими биографических данных и другой информации. Он также подтвердил свою эффективность в обнаружении

фактов воровства или иных злоупотреблений среди сотрудников. Кроме того, было установлено, что в организациях, использовавших полиграф на постоянной основе, значительно повышался уровень лояльности персонала.

Полиграф зарекомендовал себя как эффективное средство обеспечения кадровой безопасности. Эксперты доказали, что обследования на полиграфе, проводимые квалифицированными операторами, дают лучшие результаты, чем какие-либо другие методы. Кроме того, работа оператора полиграфа существенно экономит силы и время службы безопасности, значительно сужая круг подозреваемых и помогая им определить направления оперативных поисков. Практика показывает, что наличие и осознание действенности системы периодического специального контроля персонала является значимым психологическим барьером для лиц, склонных к нарушениям или легкомысленных сотрудников, допущенных к коммерческой тайне.

Психологическое тестирование и обследование на полиграфе носят добровольных характер и никаким образом не причиняют вреда здоровью тестируемых. С кандидата или сотрудника фирмы берется подписка о неразглашении им особенностей отбора на фирму, а также содержания и порядка проверки персонала учреждения, которая прикладывается к заключению и хранится в фирме у заказчика.

Чтобы оценить уровень развития профессиональных навыков, можно попросить претендента выполнить определенную «пробную» работу. Если предполагаемая работа связана с ответственностью, предложите претенденту написать план действий на новом месте. Такой план мгновенно показывает способности человека мыслить, распределять свое время, выделять приоритеты в работе и реально оценивать эффективность своих действий. Предложите одинаковые вопросы и тесты всем кандидатам без исключения. И тогда вы сможете сравнить, на что способен каждый из них. Принимая окончательное решение, важно не поддаться первому, как правило, достаточно субъективному впечатлению. Оно может быть ошибочным. Поэтому профессиональные рекрутеры (специалисты по подбору персонала) предпочитают во время собеседования вместо обычного разговора о работе проводить так называемое структурированное интервью. Интервьюер предлагает кандидату представить себя в той или иной ситуации (реальной или выдуманной) и рассказать, как он себя поведет. Ответы собеседника показывают, на что он способен.

В крупных организациях часто используются психометрические тесты. Они позволяют лучше понять особенности характера претендента. Однако иметь в штате специалиста, который мог бы обработать такой тест для небольшой организации, слишком дорого. Поэтому лучше всего воспользоваться услугами привлеченного психолога, который владеет стандартными, хорошо зарекомендовавшими себя тестами.

В заключение приведем «памятку по подбору персонала», которую удобно использовать в практической деятельности.

ПАМЯТКА ПО ПОДБОРУ ПЕРСОНАЛА

• Определите перечень навыков, которыми должны обладать кандидаты на вакантную должность. Учитывайте как профессиональный опыт, так и личные качества претендентов.

• Проведите идентификацию личности.

• Проверьте документы, подтверждающие наличие образования и ученых степеней.

• При согласии кандидата проведите его проверку на детекторе лжи.

• Используйте резюме, чтобы составить первоначальное представление о кандидате. Но окончательное решение принимайте после личной беседы.

• Не принимайте требования кандидата с первого же раза. Сначала убедитесь, справится ли он с должностными обязанностями.

• Предложите кандидату несколько тестов, чтобы проверить его компетентность.

• Предлагайте одинаковые вопросы и тесты всем претендентам без исключения. Так вы избежите упреков в дискриминации.

• Попросите кандидата представить рекомендации с предыдущей работы.

• Установите четкие критерии, по которым вы будете оценивать результаты прохождения кандидатом испытательного срока.

8.3. Требования к специалистам по защите информации

Сегодня специалисты по информационной безопасности должны обладать познаниями в следующих областях:

• Информационно-аналитическая работа.
• Методы разведки и контрразведки.
• Оперативная работа.
• Социальная психология и психология личности.
• Основы банковского дела и бухгалтерский учет.
• Основы менеджмента и маркетинга.
• Гражданское и уголовное право.

Грамотный специалист обязан [23]:

1. Разработать комплексные меры по обеспечению безопасности коммерческой фирмы и личной безопасности ее руководства.
2. Осуществить защиту конфиденциальной информации, в том числе хранящейся в компьютерной памяти, а также в локальных и распределенных сетях.
3. Уметь применять технические средства скрытого наблюдения и прослушивания.
4. Противодействовать проведению аналогичных мероприятий конкурентами.
5. Разбираться в финансовой отчетности.
6. Проводить внутреннее расследование случаев воровства, мошенничества, саботажа и финансовых преступлений.
7. Организовать проверки (в том числе негласные) благонадежности сотрудников фирмы.
8. Предупреждать (выявлять) случаи сотрудничества работников фирмы с конкурентами или криминальными структурами.
9. Взаимодействовать со следственными органами и милицией при расследовании преступлений иных происшествий.
10. Готовить документы, содержащие анализ финансово-экономического положения партнеров, оценку конкурентов и потенциальных клиентов.
11. Разрешать конфликты между сотрудниками фирмы.
12. Кратко и точно излагать свои мысли.

Анализ опыта и знаний в перечисленных областях у ведущих сотрудников многих служб безопасности отечественных коммерческих фирм, как показывают различные опросы, не соответствуют требованиям. Поэтому вопрос об их подготовке и переподготовке более чем актуален.

8.4. Организация обучения специалистов по защите информации

Обучение (или тренинг – от английского слова training – практическая подготовка, тренировка или учеба) по вопросам защиты коммерческой тайны и обеспечения безопасности фирмы позволяет достичь следующую цель: – работники фирмы становятся более грамотными и умелыми в этом вопросе, что помогает:

1. Предотвратить утечку информации из-за простой небрежности.
2. Быстро и легко выполнять текущие задачи.

3. Решать новые и более сложные задачи.

4. Противостоять промышленному шпионажу и криминальным элементам.

В США сложные программы тренингов по безопасности первоначально создавались для работников ядерной промышленности, а сейчас получают все более широкое распространение в частных фирмах и в корпорациях для работников СБ и сотрудников, имеющих дело с коммерческой тайной и в процессе работы [25]. Обычно тренинги планируют и организуют директор службы безопасности и начальник отдела управления сотрудниками фирмы, они должны суметь извлечь из тренинга максимальную выгоду (ведь практически всегда он происходит в рабочее время). Чтобы программа тренинга была успешной, она должна быть полезной, уместной, интересной, она должна отвечать и нуждам фирмы, и нуждам конкретного отдела, и нуждам каждого работника в отдельности.

Сотрудникам выдается инструкция в отношении коммерческой тайны фирмы. Каждый новый работник должен быть ознакомлен с программой защиты коммерческой тайны фирмы сотрудниками СБ.

Ориентационные семинары также имеют своей целью обучение методам сохранности ценной информации. Сотрудники должны четко знать категории охраняемых сведений, возможные способы и методы проникновения к ним со стороны нарушителя, процедуры защиты коммерческой тайны и правила работы с конфиденциальными документами и изделиями. Кроме этого, в фирмах США в программе ориентации принято затрагивать следующие вопросы [25]:

• идентификационные карточки и значки, как часто их следует носить;

• правила проноса и выноса багажа и ручной клади;

• разрешенные выходы для персонала и посетителей;

• маршруты эвакуации и действия работников в экстремальных ситуациях, запасные выходы;

• проверка личного транспорта въезжающего и выезжающего с территории фирмы, инспекция грузов и личных вещей, когда и почему она проводится.

Специальные семинары для работников соответствующих специальностей могут быть проведены по темам: обеспечение защиты информации в ЭВМ, технические средства охраны и т.д. Описанная система ориентации необходима, она формирует у работников отношение к секретам фирмы, осознание их важности.

Однако дальнейшая программа обучения не менее важна. Прежде всего надо держать сотрудников в курсе изменений в системе защиты коммерческой тайны – новых правил, положений, требований – издавать соответствующие информационные листки и бюллетени. Можно сделать информационный стенд, на котором все сведения будут ежемесячно обновляться. Подобные мероприятия не только помогут предотвратить утечку информации, но и дадут служащим повод думать, что руководство думает о них, оно заинтересовано в повышении их осведомленности и уровня знаний, что оно осознает их роль в защите секретов фирмы. Кроме того, большинству сотрудников мало объяснить требования системы защиты коммерческой тайны, а надо постоянно напоминать о них. В этой связи тренинги должны носить достаточно регулярный характер.

Особого упоминания заслуживают занятия для сотрудников СБ. В США в 80-е – начало 90-х годов бывшими сотрудниками ЦРУ был основан ряд учебных заведений, в которых ведется систематическая подготовка специалистов для специальных органов страны, а также для частных служб безопасности фирм и банков США,

Как показывает анализ программ учебных планов и курсов подобных заведений, слушателей в обязательном порядке знакомят с особенностями деятельности разведывательных служб, обучают приемам выявления работников и агентов органов разведки, разнообразным приемам обеспечения безопасности фирм и т.д.

Кроме того, на курсах изучаются следующие основные направления:

• физическая охрана объектов;
• электронные системы охраны;
• методы проверки кадрового состава;
• методы противодействия промышленному шпионажу.

Особое внимание следует обратить на обучение сотрудников, занимающихся сбытом продукции и услуг компании. Эти люди часто находятся в ситуациях, благоприятных для утечки информации. Они должны быть четко проинструктированы, что можно говорить, что нельзя. Нередки анонимные запросы от «потенциальных клиентов» с просьбой сообщить информацию об изделии для понимания того, как его применить наилучшим образом. Конкурент может выяснить существенные вещи, проанализировав эту незначительную на первый взгляд информацию и использовать ее во вред предприятию.

8.5. Требования к начальнику службы безопасности предприятия

Начальник службы безопасности является прямым начальником для всего личного состава службы.

Он непосредственно подчинен директору фирмы либо одному из его заместителей, определенному штатным расписанием или приказом по предприятию. Начальник СБП осуществляет руководство всей текущей деятельностью, решает все организационные вопросы деятельности СБ, кроме тех, которые отнесены к исключительной компетенции дирекции фирмы. При передаче дирекцией фирмы части принадлежащих ему прав в компетенцию начальника СБП он осуществляет указанные в решении дирекции фирмы функции.

Начальник СБП назначается дирекцией фирмы из лиц, имеющих высшее образование. Директор предприятия по поручению дирекции заключает с ним трудовой договор, в котором подробно оговариваются его должностные обязанности и условия труда.

Начальник СБП подотчетен директору предприятия и несет перед ним ответственность за осуществление деятельности СБ и выполнение возложенных на нее задач и функций.

Начальник СБП без достоверности действует от имени СБ во всей его деятельности, имеет право подписи всех правовых и бухгалтерских документов, определяет должностные оклады сотрудников СБП, решает вопросы о поощрениях и взысканиях, заключает трудовые договоры с сотрудниками СБП, привлекает для работы работников на основе гражданско-правовых договоров, самостоятельно определяя условия их оплаты, представляет на согласование дирекции фирмы кандидатуры на должность заместителя начальника СБП, руководителей отделов и групп.

На время своего отсутствия начальник СБП передает свои права заместителю.

Начальник службы безопасности отвечает:

• За оказание охранных и сыскных услуг в интересах безопасности своей фирмы-учредителя при строгом и точном соблюдении действующего законодательства Российской Федерации.

• Обеспечение сохранности специальных средств, оружия и боеприпасов, приобретенных фирмой.

• Качество профессиональной подготовки лиц из состава службы безопасности.

Он обязан:

• руководствоваться в своей деятельности требованиями закона "О частной детективной и охранной деятельности в Российской Федерации", другими законами и

правовыми актами Российской Федерации, нормативами устава фирмы и положения о службе безопасности;

• на себя лично и на вверенную ему службу безопасности получить лицензии на право заниматься охранной деятельностью;

• организовать несение службы подчиненными лицами и контролировать ее качество;

• принять незамедлительные меры по обеспечению сохранности вверенного имущества собственника, организовать отражение противоправных посягательств на него, на здоровье и жизнь граждан и личного состава службы безопасности; обо всех таких посягательствах и их последствиях немедленно докладывать своему непосредственному руководителю;

• обо всех случаях применения огнестрельного оружия личным составом службы немедленно уведомлять органы внутренних дел по месту применения оружия;

• немедленно уведомлять прокурора о всех случаях смерти или причинения телесных повреждений;

• представлять на подпись руководству фирмы договоры с предприятиями и организациями на услуги инкассации, заключаемые по распоряжению руководства фирмы;

• своевременно организовывать подготовку, переподготовку и повышение квалификации личного состава службы безопасности, используя для этих целей на договорной основе специализированные базы (центры, полигоны, тиры, стрельбища и т. п.) государственных либо негосударственных лицензированных учебных (образовательных) учреждений;

• организовывать в порядке, определяемом Министерством внутренних дел Российской Федерации, прохождение периодической проверки частных охранников и детективов на их пригодность к действиям, связанным с применением специальных средств и огнестрельного оружия;

• осуществлять взаимодействие с кадровыми и финансовыми органами фирмы по вопросам исчисления трудового стажа для работников службы, стажа для начисления пособий по государственному социальному страхованию, обязательности страхования на случай гибели, получения увечья или иного повреждения здоровья в связи с осуществлением охранных действий;

• контролировать сроки действия лицензий на личный состав и службу безопасности, принимать своевременные меры для их продления;

• организовать учет и обеспечить надежную сохранность оружия, боеприпасов и специальных средств;

• контролировать порядок учета, хранения, ношения и перевозки огнестрельного оружия, боеприпасов к нему и специальных средств;

• проводить служебное расследование по каждому случаю недостачи, порчи, излишков специальных средств, огнестрельного оружия и боеприпасов;

• своевременно выполнять налоговые и иные финансовые обязательства службы безопасности и контролировать соблюдение аналогичных обязательств личным составом службы;

• предоставлять уполномоченным лицам органов, контролирующих деятельность частных детективных и охранных предприятий и служб безопасности, требуемые документы, письменную и (или) устную информацию, необходимую для выполнения контрольных функций.

Начальнику службы безопасности не разрешается совмещать охранную деятельность с государственной службой либо с выборной оплачиваемой должностью в общественных объединениях, а также оказывать услуги лично или через своих подчиненных, связанных с обеспечением безопасности сторонних предприятий. По

мнению американских специалистов в области безопасности, высказанному на международной конференции "Бизнес и безопасность", для успешной работы руководителю службы безопасности требуются следующие затраты времени [12]:

1 6% - менеджмент
2 5%-организационные вопросы
3 7% - безопасность персонала
4 16% - физическая безопасность фирмы
5 7% - защита информации
6 20% - средства безопасности
7 4% - рассмотрение злоупотреблений со стороны персонала и сотрудников СБ
8 14% - предотвращение угроз
9 8% - связь с другими организациями и с органами внутренних дел
10 18% - прочие вопросы

8.6. Новые подходы к кадровому обеспечению службы информационной безопасности предприятия

По мере развития любой отечественной компании и роста стоимости ее информационных активов совершенствуется и служба информационной безопасности. Причем стратегия и тактика работы этой службы становится одной из основных функций высшего менеджмента компании. Действительно, успех политики информационной безопасности компании зависит не только от организационных и технических решений в области защиты информации, но и от эффективности кадровых решений. Итак, каков должен быть уровень компетентности специалистов современной службы информационной безопасности российской компании.

Особенно это актуально для фирм в области информационно-коммуникационных технологий. Применительно к этой сфере в последние годы сформировался новый подход к подготовке и использованию специалистов высшего уровня в области защиты информации. Для этой группы специалистов выделяются две ключевых позиции [25]:

• CISO (Chief Information Security Officer) – директор службы информационной безопасности, который отвечает главным образом за разработку и реализацию политики безопасности компании, адекватной бизнес-процессам компании.

• BISO (Business Information Security Officer) – менеджер службы информационной безопасности, который занимается практической реализацией политики ИБ на уровне подразделения, например планово-экономического отдела, службы маркетинга или автоматизации.

Рассмотрим возможную организационную структуру новой службы ИБ компании (рис. 8.1). Здесь, на наш взгляд, принципиальны следующие моменты (статусный и функциональный).

Рис. 8.1. Организационная структура службы ИБ компании [25]

Блок-схема: альтернативный процесс: BISO (Business Infonnation Security Officer)
Блок-схема: альтернативный процесс: Руководители подразделений
Блок-схема: альтернативный процесс: Обработка инцидентов:
• изучение угроз и инцидентов
• предложение адекватных решений
Блок-схема: альтернативный процесс: Техническая поддержка:
• внедрение и поддержание платформы
• техническое обеспечение архитектуры ИБ
Блок-схема: альтернативный процесс: Администрирование ИБ:
• выбор платформы
• обучение пользователей

Блок-схема: альтернативный процесс: Разработка политики:
• политики и стандарты
• оценка и определение рисков
• консультирование
• информирование руководства
• согласование регламентов
• архитектура безопасности бизнеса
Блок-схема: альтернативный процесс: CISO (Chief Infonnation Security Officer)
Блок-схема: альтернативный процесс: Исполнительный директор
Блок-схема: альтернативный процесс: Директор по IT
Блок-схема: альтернативный процесс: Совет учредителей или совет директоров

Раньше в большинстве российских компаний обеспечением информационной безопасности занимались отделы и службы автоматизации. В настоящее время ведущие отечественные компании предпочитают создавать для этих целей специальное подразделение, что, естественно, влечет организационные, кадровые и финансовые изменения, Таким образом, спрос на квалифицированных специалистов по защите информации растет.

Статус лица, определяющего защищенность информационных ресурсов компании, соответствует статусу ведущих TOP-менеджеров компании, отвечающих за развитие таких ресурсов компании, как финансовые (финансовый директор), технологические (директор по производству), человеческие (директор по персоналу) и т. д. По всей видимости, рынком будут востребованы специалисты по ИБ с мощной технической и управленческой составляющей, что традиционно является проблемой для российского рынка труда.

К аналогичным выводам пришли аналитики консалтинговой компании КПМГ, отметив, что в наиболее благополучных, с точки зрения ИБ, компаниях эта функция входит в компетенцию высшего руководства. Согласно исследованию КПМГ, почти в половине организаций ответственность за ИБ была определена на уровне совета директоров, что наиболее характерно для финансового сектора [25]. Непосредственное участие TOP-менеджмента организации необходимо для постановки правильных целей в области защиты информации, позволяющих без ущерба осуществлять деятельность и ее развитие. Руководство должно обеспечить функцию безопасности надлежащим уровнем инвестирования и ресурсов, а также оценивать ее эффективность.

Если поиск компетентного специалиста на позицию BISO – вопрос сложный, но вполне решаемый, то поиск CISO, по всей видимости, самая настоящая проблема, поскольку профиль такой компетенции не сформирован и подготовленные специалисты в России отсутствуют.

Действительно, главная задача CISO – это оценка и управление технологическими, производственными и информационными рисками компании. Роль CISO по этим вопросам предполагает, что данный специалист должен быть способен идентифицировать и управлять рисками в соответствии с целями и задачами компании и уровнем ее развития. Свою специфику вносит и сфера деятельности компании, а также ее размер и стоимость информационных активов.

CISO должен входить в верхний эшелон управления компанией и уметь сбалансировать потребности бизнеса и требования безопасности с учетом усложняющихся технологий возросшего числа действий злоумышленников и террористических актов, требований законодательства и ожиданий партнеров. Часто потребности бизнеса входят в противоречие с требованиями безопасности. CISO должен быть способен переводить с «русского на русский», то есть с технического русского на тот русский, который понятен руководителям бизнеса. Помимо солидного образования и опыта в области защиты информации (5-7 лет в области защиты информации полюс

дополнительное образование или опыт в IT), CISO, несомненно, должен обладать стратегическим складом ума, фундаментальными знаниями в управлении предприятием и лояльностью к компании. Для этого недостаточно только технического (технологического) образования, так же как и только «защитного». Позицию CISO скорее всего будут занимать аудиторы или аналитики в области безопасности. Идеально, если подобный специалист будет привлечен из числа своих же сотрудников, ибо в этом случае профессиональная компетенция усилена еще и знанием конкретного предприятия [25].

По мнению аналитиков, CISO должны быть способны выполнять следующие функции:

. разработка политики в области ИБ, включая регламенты, стандарты, руководства;

. разработка принципов классификации информационных потоков и управлении ими;

. анализ рисков, их оценка и принятие;

. обеспечение персонала всех подразделений руководствами и знаниями по исполнению политики в области ИБ, организация соответствующего обучения инструктирования;

. консультирование менеджеров компании и исполнительского персонала в пределах их компетенции по вопросам информационных рисков и защиты от них;

. согласование всех политик и регламентов с тем, чтобы они были успешно внедрены на всех уровнях компании;

. деятельность в составе рабочих групп или экспертных советов, оценивающих риски при внедрении новых технологий, модернизации производства, формировании планов технического обновления или иных изменений бизнеса. Включение аспектов ИБ на самые ранние этапы данных проектов;

. «связующее звено» между службой качества и отделом IT/автоматизации с правом проверки внутренних отчетов службы качества;

. совместная работа со службой безопасности в части, касающейся их обоих, например научно-исследовательские работы (НИОКР) или пропускная система (бейджи, пропуска);

. совместная работа со службой персонала в части, касающейся проверки некоторых данных при найме на работу;

. в случае кризисов или чрезвычайных происшествий в области защиты информации участвовать вместе с TOP-менеджментом в управлении кризисом;

. информационная поддержка TOP-менеджеров об изменениях в законодательстве и технических новинках, имеющих отношение к информационной безопасности.

Контрольные вопросы

1. Назовите виды угроз от сотрудников и нарушителей по возрастанию степени их опасности.
2. Опишите последовательность действий СБП при приеме на работу новых сотрудников.
3. Какие действия предпринимаются при нарушении персоналом информационной безопасности?
4. Как осуществляется набор персонала в СБП?
5. В чем особенность отбора персонала в СБП и последовательность его проведения.
6. Какие требования учитываются при отборе кандидатов на должность начальника СБП?
7. Опишите назначение и методы проведения тестирования при отборе персонала в СБП.

8. Какими знаниями и навыками должен владеть современный специалист по защите информации.

9. Перечислите основные обязанности начальника СБП.

10. Назовите новые подходы к организации служб информации на современных фирмах.

Методические указания по выполнению практических занятий

Содержание

Введение

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий электронных платежей и "безбумажного" документооборота серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. По статистике фирмы Infonetics, сбои в среднестатистической североамериканской локальной сети происходят 23.6 раза в течение года, и затраты на их устранение составляют в среднем около 5 часов. Потери компании - владельца сети при этом составляют от одной до пятидесяти тысяч долларов в час. При этом учитываются не только прямые затраты на ликвидацию повреждения, но и упущенная выгода, потеря рабочего времени и иной ущерб.

Данных о потерях российских компаний от сбоев в работе локальных сетей в прессе пока не приводилось, однако можно предположить, что и для них проблема отказоустойчивости сети и защиты данных является актуальной. Ведь не секрет, что многие российские фирмы на заре своей деятельности отдавали предпочтение наиболее дешевым и, зачастую, наименее надежным сетевым решениям. По данным анкетирования 100 администраторов локальных сетей, проведенного фирмой АйТи в январе этого года, серьезные сбои в работе сетевого оборудования и программного обеспечения в большинстве российских фирм происходят не реже, чем один раз в месяц.

Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.

Занятие 1. Конфигурирование прокси-сервера

Краткие теоретические сведения

Прокси-сервер

Прокси-сервер (от англ.Proxy — «представитель, уполномоченный») — служба в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Чаще всего прокси-серверы применяются для следующих целей:

- Обеспечение доступа с компьютеров локальной сети в Интернет.
- Кэширование данных: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем сам нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации.
- Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика клиента или внутреннего - компании, в которой установлен прокси-сервер.
- Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер). См. также NAT.
- Ограничение доступа из локальной сети к внешней: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы.
- Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет

возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе.

- Обход ограничений доступа. Прокси-серверы популярны среди пользователей несвободных стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

Прокси-сервер, к которому может получить доступ любой пользователь сети интернет, называется открытым.

Виды прокси-серверов

Прозрачный прокси — схема связи, при которой трафик, или его часть, перенаправляется на прокси-сервер неявно (средствами маршрутизатора). При этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек, но с другой стороны, не имеет выбора.

Обратный прокси — прокси-сервер, который в отличие от прямого, ретранслирует запросы клиентов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети. Часто используется для балансировки сетевой нагрузки между несколькими веб-серверами и повышения их безопасности, играя при этом роль межсетевого экрана на прикладном уровне.

Методические указания по выполнению работы

Начало редактирования файла

Необходимо открыть терминал с правами root (sudosu/su)

Sudoetc/squid/squid.conf

После редактирования сохранить, и прописать команду для реконфигурирования конфигурационного файла.

Squid –kreconfigure

Синтаксис конфигурациооного файла Squid.

Списки доступа (ACL)

Система управления доступом в прокси-сервере Squid является очень гибкой

и обширной. Она состоит из элементов со значениями и списков доступа с

указанием allow (разрешение) или deny (запрещение).

Формат Acl следующий:

acl имя элемент список

Формат правил доступа:

http_accessallow/denyимя_acl

Рассмотрим некоторые типы acl, которые позволяет использовать прокси-сервер Squid, конечно же с примерами:

IP-адрес источника

* acl имя src список

В следующем примере разрешим User1 и отделу программирования (Progs) доступ к прокси-серверу, а всем остальным запретим:

aclProgssrc 192.168.0.1-192.168.0.9

aclUser1src 192.168.0.10

http_access allowProgs

http_access allowUser1

http_accessdenyall

IP-адрес назначения

* acl имя dst список

IP-адрес назначения – адрес сервера к которому желает получить доступ клиент прокси-сервера.

В следующем примере запретим User1 доступ к подсети 194.67.0.0/16 (к примеру, в ней находится тот же aport.ru):

acl Net194dst 194.67.0.0/16

http_access deny User1 Net194

MAC адрес источника

Для некоторых операционных систем поддерживаются списки доступа по MAC адресаам. В Squid это называется ARP ACLs и поддерживается на Linux, Solaris и возможно для BSD вариантов.

Squid может определить MAC-адрес клиента только для своей подсети.

```
aclUser1arp 01:02:03:04:05:06
```

Домен назначения

```
acl  имя  dstdomain  список
```

Домен назначения – домен доступ к которому желает получить клиент прокси-сервера.

В следующем примере запретим User1 доступ к сайтам nnm.ru и kpnemo.ru:

```
acl  Sites1dstdomain  .nnm.ru  .kpnemo.ru

http_accessdenyUser1   Sites1
```

В случае, если будет необходимо указать домен источника, то используйте srcdomain.

Домены назначения и источника с использованием регулярных выражений

```
aclимя [-i] srcdom_regexсписок

aclимя [-i] dstdom_regexсписок
```

Данные элементы отличаются от srcdomain и dstdomain лишь тем, что в них используются регулярные выражения. Пример:

```
aclSitesRegexSexdstdom_regexsex

aclSitesRegexComNetdstdom_regex  \.com$ \.net$

http_access   deny   User1SitesRegexSex

http_access   deny   User1SitesRegexCoacl M1 arp 01:02:03:04:05:06

mNet
```

В данном примере запрещён доступ User1 на все домены, содержащие слово sex и на все домены в зонах .com и .net.

Ключ -i призван игнорировать регистр символов в регулярных выражениях.

Шаблон регулярного выражения для URL.

* aclимя [-i] url_regexсписок

Пример указания файлов с расширением avi, начинающихся на слово sex:

aclNoAviFromSexurl_regex -i sex.*\.avi$

В случае, если необходимо указать шаблон только для пути URL, то есть исключая протокол и имя хоста (домена), то используйте urlpath_regex.

Пример для указания музыкальных файлов:

acl media urlpath_regex -i \.mp3$ \.asf$ \.wma$

Указание номера порта назначения

aclимя_aclportcписок

Порт, к которому желает подключится клиент прокси-сервера.

Как пример, запретим всем использование программы Mirc через прокси-сервер:

aclMirc port 6667-6669 7770-7776

http_access deny all Mirc

Указание протокола передачи

aclимя_aclproto список

Как пример, запретим вышеупомянутомуUser1 использование протокола FTP через прокси-сервер:

aclftpproto proto ftp

http_access deny User1ftpproto

Указание метода http запроса клиентом (GET, POST).

GET, POST-методы передачи переменных

aclимя_aclmethodcписок

Возьмем ситуацию, когда необходимо запретить User1 просматривать его почту на сайте mail.ru, но при этом разрешить просматривать сайт без запретов, то есть запретить User1 возможность войти в свой почтовый ящик через форму входа на сайте:

```
aclSiteMailRudstdomain  .mail.ru
aclmethodpost  method      POST
http_access  denyUser1methodpostSiteMailRu
```

Ограничение полосы пропускания для группы пользователей

Регулировка скорости в прокси-сервере Squid осуществляется с помощью пулов.

Pool-механизм ограничения скорости загрузки. Каждый пул определяется тремя параметрами: размером буфера и скоростью его заполнения: delay_class, delay_parameters, delay_access.

1. Ограничена общая скорость загрузки.
2. Ограничена общая скорость загрузки и скорость загрузки индивидуального хоста (биты 25 -32 IP-адреса).
3. Ограничена общая скорость загрузки, скорость загузки подсети (биты 17-24 IP-адреса) и скорость загрузки индивидуального хоста (биты 25 -32 IP-адреса).

Форматы:

```
delay_poolsколичество_объявленных_пулов
delay_accessномер_пула  действие   имя_acl
```

действие может быть allow (разрешить) и deny (запретить). При этом, данный пул действует на тех, кому он разрешен и не действует на тех, кому он запрещен. В случае, если указано allowall, а затем denyUser1, то на а данный класс всё-равно подействует, т.к. IP-адрес а объявленный в aclUser1, входит в список адресов aclall. Имейте это ввиду.

```
delay_classномер_пулакласс_пула
delay_parametersномер_пула  параметры
```

параметры отличаются в зависимости от класса пула:

для первого класса:

delay_parameters 1 байт_на_всю_сеть

для второго класса:

delay_parameters 1 на_всю_сетьна_клиента

для третьего класса:

delay_parameters 1 на_всю_сетьна_подсетьна_клиента

Ограничить пользователей по времени работы в сети

acl имя time дни чч:мм-ЧЧ:ММ

Где день: M - Понедельник, T - Вторник, W - Среда, H — Четверг,
F - Пятница, A - Суббота, S — Воскресенье.

При этом чч:мм должно быть меньше чем ЧЧ:ММ, то есть можно указать с 00:00-23:59, но нельзя указать 20:00-09:00.

Настройка прозрачного прокси

Таблица N 1. Примеры различных форм задания диапазонов адресов.

Диапазон адресов	Полная форма	Краткая форма
192.168.0.1-192.168.0.254	192.168.0.0/255.255.255.0	192.168.0.0/24
192.168.20.1-192.168.20.254	192.168.20.0/255.255.255.0	192.168.20.0/24
192.168.0.1-192.168.254.254	192.168.20.0/255.255.0.0	192.168.20.0/16
10.0.0.1-10.254.254.254	10.0.0.0/255.0.0.0	10.0.0.0/8

Порядок чтения конфигурационного файла

Конфигурационный файл читается сверху вниз. Правила применяются последовательно в порядке их задания в конфигурационном файле. Правило первое правило удовлетворяющее условию запроса будет выполнено, а последующие будут проигнорированны.

Логические операции И/ИЛИ в списках доступа

Эти операции уже встроены в схему контроля доступа, их необходимо учитывать при написании конфигурационного файла.

- Все элементы, указанные в данном*acl* объединяются при помощи логического ИЛИ.
- Все элементы, указанные в *access* объединяются при помощи логического И.

Например, следующая конфигурация контроля доступа никогда не будет работать:

acl ME src 10.0.0.1

acl YOU src 10.0.0.2

http_accessallow ME YOU

Для того, чтобы запрос был разрешен, он должен совпасть и с acl ``ME" И acl ``YOU". Это невозможно, т.к. IP-адрес в данном случаю может совпасть либо с одним, либо с другим acl. Это должно быть заменено на:

acl ME src 10.0.0.1

acl YOU src 10.0.0.2

http_access allow ME

http_access allow YOU

Такая конструкция тоже должна работать:

acl US src 10.0.0.1 10.0.0

http_access allow US

Порядок выполнения работы

Создание исходной конфигурации

В учебном классе существует сеть с адресами от 192.168.2.17 до 192.168.2.31. Обозначим диапазон адресов указанной подсети именем *localnet.* Дляэтого добавим в конфигурационный файл новую запись, создающую Acl (см. таблицу N1):

acllocalnetsrc 192.168.2.16/28

Прокси-сервер Squid расположен на сервере S10, IP-адрес которого 192.168.2.24. Squid использует стандартный порт 3128. Для корректной работы Squid необходимо в его конфигурационном файле указать эти данные следующим образом:

http_port 192.168.2.24:3128

Для того, чтобы пользователи других сетей не могли использовать имеющийся канал Интернет, целесообразно запретить им доступ к прокси-серверу следующим образом:

http_access allow localnet

http_access deny all

Будьте внимательны, указывая http_access, так как Squid использует их в порядке указания Вами.

Задания для самостоятельного выполнения

Запретить доступ к заданному домену для всех пользователей сети

Определить aclсодержащий всю сеть

acllocalnetsrc 192.168.0.0/16

Определитьaclсодержащий запрещённые домены

aclDenyDomaindstdomainvkontakte.ruporno.com

Запрещаем доступ из локальной сети к этим доменам

http_accessdenylocalnetDenyDomain

Запретить доступ к заданному домену для некоторых пользователей сети

Определитьacl содержащий список пользователей

aclUserssrc 192.168.0.5 192.168.0.6 192.168.0.15

Запрещаем этим пользователям доступ к доменам

http_accessdenyUsersDenyDomain

Запретить доступ для пользователя по его MAC адрес

aclUser1arp 01:02:03:04:05:06

http_access deny User1DenyDomain

Запретит доступ ко всем поддоменам домена

Определитьacl содержащий список доменов. Обратите внимание на **точку** перед адресом домена.

aclDenyDomaindstdomain .mail.ru

Запрещаем доступ из нашей сети к этим доменам и их поддоменам

http_accessdenylocalnetDenyDomain

Фильтрация загрузки контента страницы

Для того что бы запретить пользователю загружать не всю страницу а лишь конкретный контент (например рекламный баннер), необходимо указать URL с которого он загружается и запретить загрузку с этого адреса.

Для этого открываем страницу в HTMLформате и анализируем содержание.

Часто случается так что рекламные баннеры лежат на отдельном домене содержащем рекламные баннеры, то можно закрыть весь домен как было показано выше.

aclMailRuurl_regex -i rs.mail.ru/n87281440.gif

Эта конструкция поддерживает регулярные выражения, это позволяет заблокировать все изображения в формате .gif с сайта rs.mail.ru следующим образом

aclMailRuurl_regex -i rs.mail.ru/[a-z][0-9]*\.gif

Ключ -i позволяет не обращать внимания на регистр.

Разделение общего канала на несколько пулов

Для примера, у нас канал на 32000Кбит (в среднем 15000Кбайт в секунду) и

желаем User1 дать всего 4000Кбайта/сек, отделу программирования (Prog) дать всего 10000

Кбайт/сек и на каждого всего по 5000 Кб/сек (всего два бокальчика), всех

остальных ограничить в 2000Кбайта/сек на каждого и 10000 Кб/сек на всех, а

файлы mp3 (media) ограничить в 3000 Кбайта в секунду на всех. Тогда пишем:

aclProgsrc 192.168.0.1-192.168.0.9

aclUser1src 192.168.0.10

acllocalnetsrc 192.168.0.0/255.255.255.0

```
acl media   urlpath_regex -i \.mp3$ \.asf$ \.wma$


delay_pools 4
# сначалаограничиммедиафайлы
delay_class 1 1
delay_parameters 1 3000/3000
delay_access 1 allow media
delay_access 1 deny all
# Ограничим пользователя User1
delay_class 2 1
delay_parameters 2 4000/4000
delay_access 2 allow User1
delay_access 2 denyall
# ограничим отдел программирования
delay_class 3 2
delay_parameters 3 10000/10000 5000/5000
delay_access 3 allow Prog
delay_access 3 denyall
#ограничим остальных (второй класс пула)
delay_class 4 2
delay_parameters 4 10000/10000  2000/2000
delay_access 4 deny media
delay_access 4 deny User1
delay_access 4 deny Prog
delay_access 4 allow localnet
delay_access 4 deny all
```

Невозможно средствами Squidразделить канал между всеми активными пользователями.

delay_class 1 2

delay_parameters 1 -1/-1 5000/15000

delay_access 1 allow localnet

delay_access 1 deny all

Зададимнавсюсеть и на подсети максимальный канал (-1 означает неограниченность), а каждому пользователю зададим максимальную скорость в 5000 Кб/сек после того, как пользователь скачает на максимальной скорости первые 15 Кбайт документа.

Таким образом клиент не использует весь канал, но достаточно быстро получит первые 15 Кбайт.

Задать временные промежутки для пользователя

Запретим всё тому же User1 иметь доступ в сеть Интернет с 10 до 15 часов каждый день:

acl TimeUser1 time 10:00-15:00

http_accessdenyUser1 TimeUser1

Для того, чтобыUser1 мог пользоваться программой Mirc с 13 до 14 часов:

acl TimeUser1 time 13:00-14:00

http_access allowUser1 TimeUser1Mirc

http_accessdenyUser1Mirc

Просмотр статистики Sarg

Для проверки статистикив браузере на прокси-сервере ввести:

Localhost/sarg/

Занятие 2. Полномочное разграничение доступа

Цель работы

Целью выполнения работы является регистрация в системе «Secret Net» ключей для администратора и одного пользователя; задание настроек входа в систему.

Краткие теоретические сведения

В системе Secret Net 6 информационная безопасность компьютеров обеспечивается механизмами защиты. Механизм защиты — совокупность настраиваемых программных средств, разграничивающих доступ к информационным ресурсам, а также осуществляющих контроль действий пользователей и регистрацию событий, связанных с информационной безопасностью.

Функциональные возможности Secret Net 6 позволяют администратору безопасности решать следующие задачи:

• усилить защиту от несанкционированного входа в систему;

• разграничить доступ пользователей к информационным ресурсам на основе

принципов избирательного и полномочного разграничения доступа и замкнутой программной среды;

• контролировать и предотвращать несанкционированное изменение целостности ресурсов;

• контролировать вывод на печать конфиденциальной информации;

• контролировать аппаратную конфигурацию защищаемых компьютеров и предотвращать попытки ее несанкционированного изменения;

• загружать системные журналы для просмотра сведений, произошедших на защищаемых компьютерах;

• не допускать восстановление информации, содержавшейся в удаленных файлах;

• управлять доступом пользователей к сетевым интерфейсам компьютеров.

Для решения перечисленных и других задач администратор безопасности использует средства системы Secret Net 6 и операционной системы (ОС) Windows.

Основными функциями администратора безопасности являются:

• настройка механизмов защиты, гарантирующая требуемый уровень безопасности ресурсов компьютеров;

• контроль выполняемых пользователями действий с целью предотвращения нарушений информационной безопасности.

Организация управления системой защиты

В автономном режиме функционирования системы Secret Net 6 доступны только локальные функции управления системой.

В сетевом режиме функционирования доступны возможности как локального, так и централизованного управления системой защиты, применяются принципы сетевого администрирования с использованием механизма групповых политик и делегирования административных полномочий.

В сетевом режиме функционирования системы Secret Net 6 для настройки механизмов защиты используются стандартные средства управления компьютерами и доменом, функциональные возможности которых расширяются в результате модификации схемы Active Directory (AD) и установки компонентов Secret Net 6.

Централизованное управление — управление работой системы Secret Net 6, осуществляемое администратором безопасности со своего рабочего места. Рабочим местом администратора безопасности может быть любой компьютер сети с установленными средствами централизованного управления ОС Windows. На контроллере домена средства централизованного управления установлены по умолчанию. На других компьютерах установку средств необходимо выполнить самостоятельно:

• для ОС Windows 7 — устанавливается компонент "Средства удаленного администрирования сервера для Windows 7". После установки необходимо открыть список компонентов Windows и в папке "Средства удаленного администрирования сервера" включить функции "Средства администрирования возможностей | Средства управления групповыми политиками" и "Средства администрирования ролей | Средства доменных служб Active Directory и служб Active Directory облегченного доступа к каталогам | Средства доменных служб Active Directory | Центр администрирования Active Directory";

• для ОС Windows 2008 — в списке компонентов Windows необходимо включить функции "Управление групповой политикой" и "Средства удаленного администрирования сервера | Средства администрирования ролей | Средства AD DS и AD LDS | Инструменты AD DS | Оснастки AD DS и средства командной строки" (вариант англоязычного названия: "Remote Server Administration Tools | Role Administration Tools | Active Directory Domain Services Tools | Active Directory Domain Controller Tools");

• для ОС Windows Vista — устанавливается компонент "Средства администрирования удаленного сервера для Windows Vista". После установки необходимо открыть список компонентов Windows и в папке "Средства удаленного администрирования сервера" включить функции "Средства администрирования возможностей | Средства управления групповыми политиками" и "Средства администрирования ролей | Средства доменных служб Active Directory Средства контроллеров доменов Active Directory";

• для ОС Windows XP/2003 — устанавливается компонент "Microsoft Administration Tools Pack" из состава дистрибутива ОС Windows 2003 Server;

• для ОС Windows 2000 — устанавливается компонент "Microsoft Administration Tools Pack" из состава дистрибутива ОС Windows 2000 Server.

Локальное управление — это управление работой механизмов защиты отдельного компьютера, которое осуществляется администратором безопасности непосредственно на каждом компьютере. Локальное управление применяется в тех случаях, когда централизованно настроить механизмы защиты на отдельном компьютере (или компьютерах) по каким-либо причинам невозможно или нецелесообразно. Кроме того, локальное управление применяется для обеспечения требуемого уровня безопасности в работе локальных пользователей.

Для выполнения функций централизованного управления администратор безопасности должен входить в группу администраторов домена. Для локального — в локальную группу администраторов компьютера.

Централизованное управление имеет приоритет перед локальным управлением.

Если в групповой политике какие-то параметры для данного компьютера заданы централизованно, то локально их изменить нельзя.

В соответствии с концепцией Secret Net 6 управление безопасностью в защищаемом домене рекомендуется осуществлять централизованно. Однако следует иметь в виду, что не все параметры защитных механизмов настраиваются централизованно. Некоторые параметры могут настраиваться только локально.

В сетевом режиме функционирования системы Secret Net 6 параметры объектов групповых политик хранятся на контроллерах домена и передаются на защищаемые рабочие станции и серверы, где применяются в соответствии с действием механизма групповых политик.

Если для всех компьютеров домена используется единая политика безопасности, настройку механизмов Secret Net 6 рекомендуется выполнять в политике, применяемой к домену по умолчанию.

С помощью групповых политик для компьютеров отдельных организационных подразделений (Organization Units) домена можно задавать особые параметры механизмов защиты, отличающиеся от общих параметров, применяемых в домене. В общем случае последовательность формирования политик, применяемых к организационным подразделениям, следующая:

1. Настройте механизмы защиты Secret Net 6 в рамках доменной политики.

2. Создайте в домене новые организационные подразделения, для которых должны действовать особые параметры механизмов защиты.

3. Добавьте в созданные подразделения нужные компьютеры домена.

4. Создайте для каждого подразделения свою групповую политику и настройте нужным образом в каждой политике параметры Secret Net 6.

5. Примените созданные политики к соответствующим подразделениям.

Инструменты Gpupdate и SecEdit. Эти инструменты командной строки позволяют принудительно обновить групповые политики для компьютера или пользователя. Эти команды могут использоваться для принудительного завершения сеанса пользователя или для перезапуска компьютера после обновления групповой политики, что полезно при обновлении политик, которые применяются только при входе пользователя в систему или при перезапуске компьютера.

Делегирование административных полномочий

В сетевом режиме функционирования системы Secret Net 6 предусмотрено де легирование полномочий администратора безопасности. Это означает, что не которые функции по настройке и управлению работой механизмов защиты могут быть возложены на пользователей, не являющихся членами доменной группы администраторов. При этом настройка и управление будут осуществ ляться только в рамках определенных организационных подразделений, соз данных внутри домена.

Для делегирования полномочий администратора безопасности необходимо вы полнить следующие действия:

1. Создать в Active Directory структуру организационных подразделений, ис пользуя стандартные средства операционной системы.

2. Пользователям, уполномоченным настраивать механизмы защиты в рамках

организационного подразделения, стандартными средствами ОС предоста вить полные права на управление объектами, входящими в подразделение, и групповыми политиками подразделения.

В результате такие пользователи получают возможность:

• управлять объектами "пользователь" и "компьютер", входящими в соот ветствующее организационное подразделение;

• редактировать (включая создание и удаление) групповые политики, на значенные для данного подразделения (обязательным условием являет ся включение пользователя в группу Group Policy Creator Owners).

3. Включить пользователя, которому делегированы права на управление объ ектами организационного подразделения, в группу SecretNetAdmins.

Эта группа создается в домене автоматически при установке Secret Net 6.

В результате пользователь в дополнение к управлению стандартными объ ектами организационного подразделения получит возможность изменять и

настраивать параметры механизмов защиты Secret Net 6:

• управлять параметрами пользователей и выполнять операции с их пер сональными идентификаторами (кроме доступа к компьютерам с ПАК "Соболь");

• редактировать параметры групповых политик данного организационно го подразделения;

• настраивать параметры контроля целостности и замкнутой программной среды для компьютеров организационного подразделения;

• устанавливать клиентское ПО Secret Net 6 в сетевом режиме функцио нирования на компьютеры, входящие в организационное подразделе ние, и настраивать параметры их подключения к серверу безопасности.

Для того чтобы пользователь, не входящий в доменную группу администраторов, мог локально выполнять настройку Secret Net 6, он должен входить в локальную группу администраторов компьютера. Кроме того, должны быть выполнены следующие условия:

• пользователю предоставлены полные права на доступ к объектам органи зационного подразделения, в которое входит данный компьютер;

• пользователь включен в группу SecretNetAdmins.

Полномочия для локального управления предоставляют следующие возможности:

• подключение и отключение ПАК "Соболь";

• изменение учетной записи компьютера;

• установка клиентского ПО Secret Net 6.

Подготовка к работе

Для выполнения работы используются компьютеры (как минимум – два), на которых установлен клиент «Secret Net». При этом на одном из них должен быть установлен и настроен компонент «Secret Net 6 – Сервер безопасности».

При подготовке к выполнению заданий изучить главы 1-2 документа ***«Secret Net 6 Руководство администратора. Управление. Основные механизмы защиты»***.

Перед началом выполнения этапа следует получить у лаборанта два ключа iButton, подписанных «Администратор» и «Пользователь».

Порядок выполнения работы

1. С рабочего места, на котором установлен и настроен компонент «Secret Net 6 – Сервер безопасности» войти в систему под учетной записью администратора, введя с клавиатуры имя пользователя и пароль.
2. Загрузить оснастку для управления параметрами пользователей, вызвать окно настройки свойств любого пользователя и перейти к диалогу «Secret Net 6».
3. Инициализировать идентификатор «Администратор».
4. Присвоить идентификатор «Администратор» учетной записи администратора системы с записью в него пароля и закрытого ключа.

5. Вывести на экран сведения о том, кому в настоящий момент принадлежит идентификатор «Пользователь». Если соответствующие сведения имеются, то следует произвести удаление идентификатора.
6. Присвоить идентификатор «Пользователь» учетной записи студента, с записью в него пароля и закрытого ключа.
7. Завершить сеанс работы в Windows.
8. Убедиться, что в идентификаторы записана вся необходимая информация. Для этого поочередно выполнить вход в систему с помощью идентификаторов «Пользователь» и «Администратор». После каждого входа проверять, под какой учетной записью выполнен вход в Windows.
9. Убедиться, что идентификаторы «Пользователь» и «Администратор» могут использоваться на клиентских машинах. Для этого рабочего места, на котором установлен и настроен клиент «Secret Net», произвести входы в систему с предъявлением идентификаторов.
10. С помощью оснастки «Конфигурация компьютера | Политики | Конфигурация Windows | Параметры безопасности | Параметры Secret Net» произвести конфигурирование механизма защиты входа в систему. Для этого следует установить следующие параметры:

- установить *запрет* вторичного входа в систему;
- установить количество неудачных попыток аутентификации равным *трём*;
- установить максимальный период неактивности до блокировки экрана равным *5 минутам*;
- установить режим *усиленной аутентификации* по ключу;
- установить режим входа пользователя в систему только по ключу.

11. Произвести смену закрытого ключа администратора с сохранением старого ключа.
12. Установить следующие параметры смены ключей:

- максимальный срок действия – 90 дней;
- минимальный срок действия – 7 дней;
- время предупреждения об истечении срока действия ключа – 3 дня.

13. После подготовки материала для оформления отчета удалить из системы информацию об идентификаторах и установить значения параметров, измененные в вышестоящих пунктах, по умолчанию.

Требования к содержанию и оформлению отчета

С отчете следует описать ход выполнения работы, обращая особое внимание на указание конкретных значений параметров системы, которые задаются в процессе выполнения работы. Привести описание результатов проверки работы при заданных значениях параметров безопасности. Для этого, например, следует производить попытки выполнения тех действий, которые были запрещены введенной политикой защиты входа в систему.

Занятие 3. Конфигурирование IDS Snort

Цель работы

Изучить основные способы сетевого сканирования компьютера на примере сканера Nmap с целью получения различной информации, а также обучиться работе с IDS Snort для обнаружения сканирования.

Теоретические сведения

Сетевое сканирование целевой системы достаточно часто используется злоумышленниками при попытках взлома. При этом основной его целью является сбор как можно большей информации о компьютере и сетевом оборудовании жертвы (причём может сканироваться как отдельный домашний компьютер, так и целая сеть предприятия): версия и тип ОС, открытые порты и типы сетевых служб на них, поддерживаемые хостом протоколы и т.д. Но также такого рода сканирование может применяться и специалистами по информационной безопасности для выявления уязвимых мест целевой системы (т.н. пентестинг).

Одной из наиболее хорошо зарекомендовавших себя программ для проведения сетевого сканирования является Nmap (даже Тринити использует её) – свободная кроссплатформенная утилита, написанная на C/C++ и Python. При выполнении данной лабораторной работы предполагается использовать именно её. Далее будут приведено краткое описание устройства некоторых сетевых технологий и методов сканирования, основанных на них.

1. Базовые сведения о TCP/IP протоколе

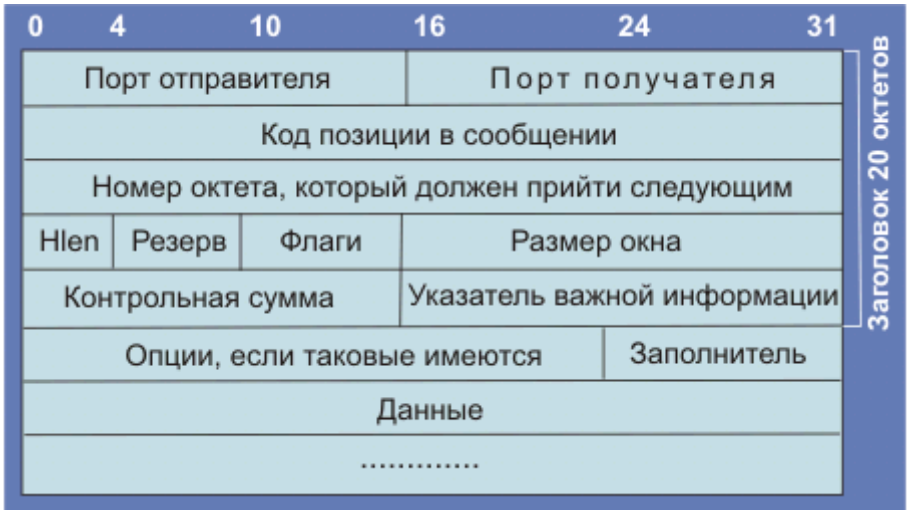
Протокол TCP (transmissioncontrolprotocol, RFC-793, -1323, -1644[T/TCP], -2018, -2581, -2582[RENO], -2861, -2873, -2883[SACK], -2923[MTU], -2988[RTO], -3293[GSMP], -3448[TFRC], -3465, -3481) в отличии от UDP осуществляет доставку дейтаграмм, называемых сегментами, в виде байтовых потоков с установлением соединения. Протокол TCP применяется в тех случаях, когда требуется гарантированная доставка сообщений. Он использует контрольные суммы пакетов для проверки их целостности и освобождает прикладные процессы от необходимости таймаутов и повторных передач для обеспечения надежности. Для отслеживания подтверждения доставки в TCP реализуется алгоритм "скользящего" окна. Подобно UDP прикладные процессы взаимодействуют с модулем TCP через порты. Под байтовыми потоками подразумевается то, что один примитив, например, read или может вызвать посылку адресату последовательности сегментов, которые образуют некоторый блок данных (сообщение). Использование портов открывает возможность осуществлять несколько соединений между двумя сетевыми объектами (работать с разными процессами).

Если IP-протокол работает с адресами, то TCP, также как и UDP, с портами. Именно с номеров портов отправителя и получателя начинается заголовок TCP-сегмента. 32-битовое поле код позиции в сообщении определяет порядковый номер первого октета в поле данных пользователя. В приложениях передатчика и приемника этому полю соответствуют 32-разрядные счетчики числа байт, которые при переполнении обнуляются. При значении флага syn=1 в этом поле лежит код ISN (InitialSequenceNumber;

смотри ниже описание процедуры установления связи), выбираемый для конкретного соединения. Первому байту, передаваемому через созданное соединение, присваивается номер ISN+1. Значение ISN может задаваться случайным образом. Но в UNIX BSD при загрузке ОС ISN делается равным 1 (это нарушает требования RFC и может использоваться для определения ОС), а далее увеличивается на 640000 каждые полсекунды. Аналогичная инкрементация осуществляется при установлении нового соединения. В RFC рекомендуется увеличивать счетчик ISN на 1 каждые 4 микросекунды.

32-битовое поле номер октета, который должен прийти следующим содержит код, который на единицу больше номера номера последнего успешно доставленного (принятого) байта. Содержимое этого поля интерпретируется получателем сегмента, только если присутствует флаг ACK. В заголовках всех сегментов, передаваемых после установления соединения это поле заполняется, а флаг ACK=1.

Поле HLEN - определяет длину заголовка сегмента, которая измеряется в 32-разрядных словах. Это поле нужно, так как в заголовке могут содержаться поля опций переменной длины. Далее следует поле резерв, предназначенное для будущего использования, в настоящее время должно обнуляться. Поле размер окна сообщает, сколько октетов готов принять получатель (флаг ACK=1) вслед за байтом, указанным в поле номер октета, который должен прийти следующим. Окно имеет принципиальное значение, оно определяет число сегментов, которые могут быть посланы без получения подтверждения. Значение ширины окна может варьироваться во время сессии (смотри описание процедуры "медленного старта"). Значение этого поля равное нулю также допустимо и указывает, что байты вплоть до указанного в поле номер октета, который должен прийти следующим, получены, но адресат временно не может принимать данные. Разрешение на посылку новой информации может быть дано с помощью посылки сегмента с тем же значением поля номер октета, который должен прийти следующим, но ненулевым значением поля ширины окна. Поле контрольная сумма предназначено для обеспечения целостности сообщения. Контрольное суммирование производится по модулю 2**32. Перед контрольным суммированием к TCP-сегменту добавляется псевдозаголовок, как и в случае протокола udp, который включает в себя адреса отправителя и получателя, код протокола и длину сегмента, исключая псевдозаголовок. Поле указатель важной информации представляет собой указатель последнего байта, содержащий информацию, которая требует немедленного реагирования. Поле имеет смысл лишь при флаге URG=1, отмечающем сегмент с первым байтом "важной



информации". Значение разрядов в 6-битовом коде флаги описано в таблице 4.4.3.1. Если флаг ACK=0, значение поля номер октета, который должен прийти следующим, игнорируется. Флаг URG=1 устанавливается в случае нажатия пользователем клавиш Del или Ctrl-C.

Рисунок 1. Устройство TCP-фрагмента

Флаги в TCP-фрагменте имеют следующее значение:

URG	Флаг важной информации, поле *Указатель важной информации* имеет смысл, если urg=1.
ACK	Номер октета, который должен прийти следующим, правилен.
PSH	Этот сегмент требует выполнения операции push. Получатель должен передать эти данные прикладной программе как можно быстрее.
RST	Прерывание связи.
SYN	Флаг для синхронизации номеров сегментов, используется при установлении связи.
FIN	Отправитель закончил посылку байтов.

Поле данные в TCP-сегменте может и отсутствовать, характер и формат передаваемой информации задается исключительно прикладной программой, теоретически максимальный размер этого поля составляет в отсутствии опций 65495 байт (на практике, помимо MSS, нужно помнить, например, о значении MTU для Ethernet, которое немногим больше 1500 байт). TCP является протоколом, который ориентируется на согласованную работу ЭВМ и программного обеспечения партнеров, участвующих в обмене информацией.

Установление связи клиент-сервер (т.н. TCPhandshake) осуществляется в три этапа:

1. Клиент посылает SYN-сегмент с указанием номера порта сервера, который предлагается использовать для организации канала связи (activeopen).

2. Сервер откликается, посылая свой SYN-сегмент, содержащий идентификатор (ISN - InitialSequenceNumber). Начальное значение ISN не равно нулю. Процедура называется passiveopen.

3. Клиент отправляет подтверждение получения SYN-сегмента от сервера с идентификатором равным ISN (сервера)+1.

Стандартная процедура установления связи представлена на рисунке 2 (под словом “стандартная” подразумевается отсутствие каких-либо отклонений от штатного режима, например, одновременного открывание соединения со стороны сервера и клиента). Если же соединение одновременно инициируется клиентом и сервером, в конечном итоге будет создан только один виртуальный канал.

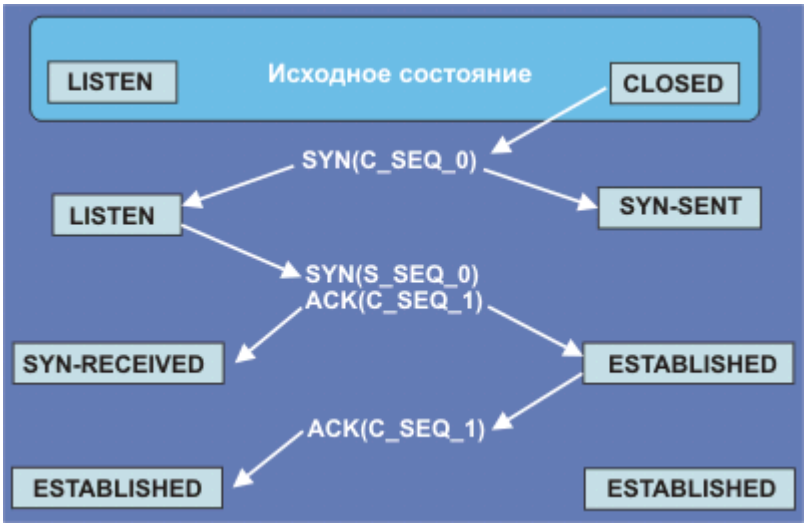
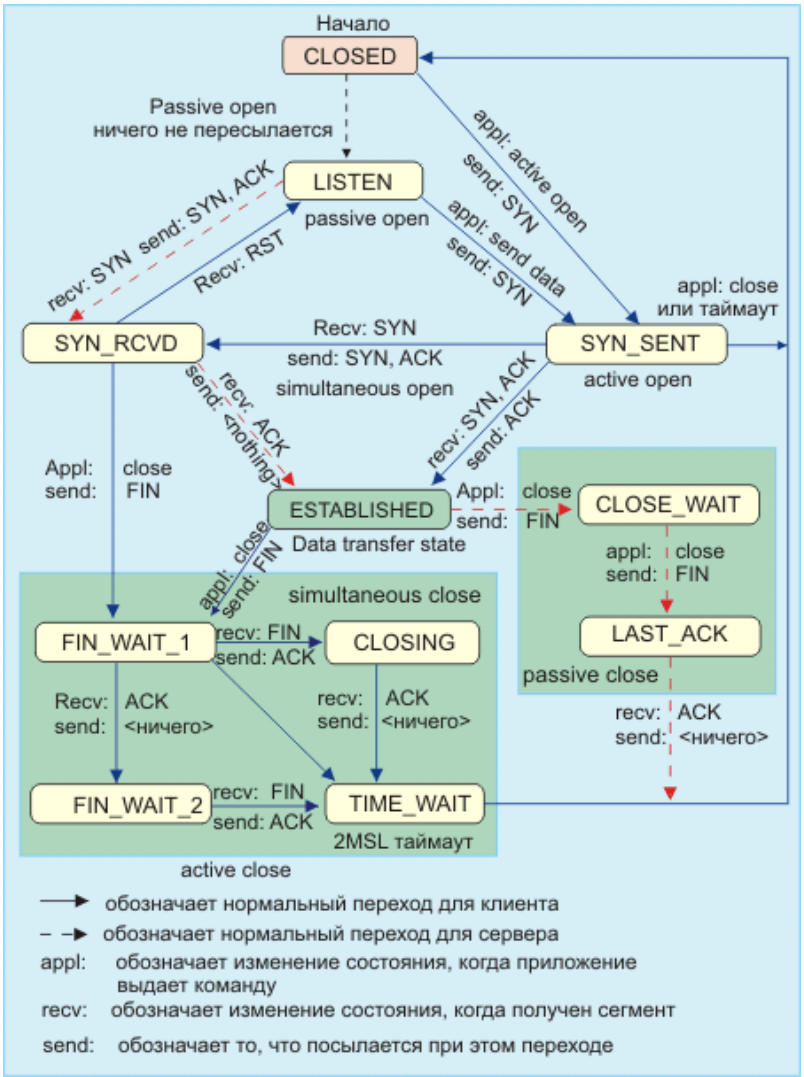


Рисунок 2. TCPhandshake



Префикс **S** на этом рисунке указывает на сервер, а **C** - на клиента. Параметры в скобках обозначают относительные значения ISN. После установления соединения ISN(S) = s_seq_1, а ISN(C) = c_seq_1.

Каждое соединение должно иметь свой неповторимый код ISN. Для реализации режима соединения прикладная программа на одном конце канала

устанавливается в режим пассивного доступа ("passiveopen"), а операционная система на другом конце ставится в режим активного доступа ("activeopen"). Протокол TCP предполагает реализацию 11 состояний (established, closed, listen, syn_sent, syn_received и т.д.; см. также RFC-793), переход между которыми строго регламентирован. Машина состояний для протокола TCP может быть описана диаграммой, представленной на рис. 3. Здесь состояние closed является начальной и конечной точкой последовательности переходов. Каждое соединение стартует из состояния closed. Из диаграммы машины состояний видно, что ни одному из состояний не поставлен в соответствие какой-либо таймер. Это означает, что машина состояний TCP может оставаться в любом из состояний сколь угодно долго. Исключение составляет keep-alive таймер, но его работа является опционной, а время по умолчанию составляет 2 часа. Это означает, что машина состояния может оставаться 2 часа без движения. В случае, когда две ЭВМ (C и S) попытаются установить связь друг с другом одновременно, реализуется режим simultaneousconnection (RFC-793). Обе ЭВМ посылают друг другу сигналы SYN. При поучении этого сигнала партнеры посылают отклики SYN+ACK. Обе ЭВМ должны обнаружить, что SYN и SYN+ACK относятся к одному и тому же соединению. Когда C и S обнаружат, что SYN+ACK соответствует посланному ранее SYN, они выключат таймер установления соединения и перейдут непосредственно в состояние syn_recvd (смотрите рисунок3).

Рисунок 3. Машина состояний TCP

2. Основные способы сетевого сканирования на примере Nmap

Nmap (“Network Mapper”) – это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Nmap использует IP пакеты, чтобы определить, какие хосты доступны в сети, какие службы (название приложения и версию) они предлагают, какие операционные системы (и версии ОС) они используют, какие типы пакетных фильтров/брандмауэров используются и еще дюжины других характеристик. В тот время как Nmap обычно используется для проверки безопасности, многие сетевые и системные администраторы находят ее полезной для обычных задач, таких как контролирование структуры сети, управление расписаниями запуска служб и учет времени работы хоста или службы.

Выходные данные Nmap это список просканированных целей с дополнительной информацией по каждой в зависимости от заданных опций. Ключевой информацией является “таблица важных портов”. Эта таблица содержит номер порта, протокол, имя службы и состояние. Состояние может иметь значение open (открыт), filtered (фильтруется), closed (закрыт) или unfiltered (не фильтруется). Открыт означает, что приложение на целевой машине готово для установки соединения/принятия пакетов на этот порт. Фильтруется означает, что брандмауэр, сетевой фильт или какая-то другая помеха в сети блокирует порт, и Nmap не может установить открыт этот порт или закрыт. Закрытые порты не связаны ни с каким приложение, так что они могут быть открыты в любой момент. Порты расцениваются как не фильтрованные, когда они отвечают на запросы Nmap, но Nmap не может определить открыты они или закрыты. Nmap выдает комбинации открыт|фильтруется и закрыт|фильтруется, когда не может определить, какое из этих двух состояний описывает порт. Эта таблица также может предоставлять детали о версии программного обеспечения, если это было запрошено. Когда осуществляется сканирование по IP протоколу (-sO), Nmap предоставляет информацию о поддерживаемых IP протоколах, а не об открытых портах.

Основными командами данной утилиты являются:

-sS (TCP SYN сканирование)

SYN это используемый по умолчанию и наиболее популярный тип сканирования. На то есть несколько причин. Он может быть быстро запущен, он способен сканировать тысячи портов в секунду при быстром соединении, его работе не препятствуют ограничивающие бранмауэры. Этот тип сканирования относительно ненавящив и незаметен, т.к. при таком сканировании TCP соединение никогда не устанавливается до конца. Он работает с любым TCP стеком, не завися от каких-либо особенностей специфичной платформы, как это происходит при сканированиях типа FIN/NULL/Xmas, Maimon и idle сканировании. Он также предоставляет ясную и достоверную дифференциацию между состояниями открыт, закрыт и фильтруется.

Эту технику часто называют сканированием с использованием полуотрытых соединений, т.к. при нём открываются полные TCP соединения, а простопосылается SYN

пакет, как установлении реальное соединение. Ответы SYN/ACK указывают на то, что порт прослушивается (открыт), а RST (сброс) на то, что не прослушивается. Если после нескольких запросов не приходит никакого ответа, то порт помечается как фильтруемый. Порт также помечается как фильтруемый, если в ответ приходит ICMP сообщение об ошибке недостижимости (тип 3, код 1,2, 3, 9, 10 или 13).

-sT (TCP сканирование с использованием системного вызова connect)

Это используемый по умолчанию тип TCP сканирования, когда недоступно SYN сканирование. Это происходит в случае, когда у пользователя нет привилегий для использования сырых пакетов или при сканировании IPv6 сетей. Вместо того чтобы использовать сырые пакеты, как это происходит при большинстве других типов сканирования, Nmap "просит" операционную систему установить соединение с целевой машиной по указанному порту путем системного вызова connect. Это такой же высокоуровневый системный вызов, используемый браузерами, P2P клиентами и другими приложениями для установки соединения. Этот вызов является частью программируемого интерфейса, известного как BerkeleySockets API. Вместо того, чтобы считывать ответы в форме сырых пакетов, Nmap использует этот API для получения информации о статусе каждой попытки соединения.

При доступности SYN сканирования, оно, безусловно, будет являться лучшим выбором, т.к.уNmap имеется меньше возможностей контролирования высокоуровнего вызова connect по сравнению с сырыми пакетами, что делает его менее эффективным. Системный вызов завершает соединения по открытым портам, вместо того, чтобы использовать полуоткрытые соединения, как в случае с SYN сканированием. Таким образом на получение той же самой информации потребуется больше времени и пакетов, да к тому же целевые машины скорее всего запишут это соединение в свои логи. То же самое сделает и порядочная IDS, хотя большинство машин не имеют такой системы защиты. Многие службы на целевой системе будут добавлять запись в системный лог (syslog), а также сообщение об ошибке, когда Nmap будет устанавливать и закрывать соединение без отправления данных. Некоторые службы могут даже аварийно завершить свою работу, когда это происходит, хотя это не является обычной ситуацией.

-sU (Различные типы UDP сканирования)

В то время как большинство сервисов Интернета используют TCP протокол, UDP службы также широко распространены. Тремя наиболее популярными являются DNS, SNMP и DHCP (используют порты 53, 161/162 и 67/68). Т.к. UDP сканирование в общем случае медленнее и сложнее TCP, то многие специалисты по безопасности игнорируют эти порты. Это является ошибкой, т.к. существуют UDP службы, которые используются атакующими. К счастью, Nmap позволяет инвентаризировать UDP порты.UDP сканирование запускается опцией -sU. Оно может быть скомбинировано с каким-либо типом TCP сканирования, например SYN сканирование (-sS), чтобы использовать оба протокола за один проход.

UDP сканирование работает путем посылки пустого (без данных) UDP заголовка на каждый целевой порт. Если в ответ приходит ICMP ошибка о недостижимости порта (тип 3, код 3), значит порт закрыт. Другие ICMP ошибки недостижимости (тип 3, коды 1, 2, 9,

10 или 13) указывают на то, что порт фильтруется. Иногда, служба будет отвечать UDP пакетом, указывая на то, что порт открыт. Если после нескольких попыток не было получено никакого ответа, то порт классифицируется как открыт|фильтруется. Это означает, что порт может быть открыт, или, возможно, пакетный фильтр блокирует его. Функция определения версии (-sV) может быть полезна для дифференциации действительно открытых портов и фильтруемых.

Большой проблемой при UDP сканировании является его медленная скорость работы. Открытые и фильтруемые порты редко посылают какие-либо ответы, заставляя Nmap отправлять повторные запросы, на случай если пакеты были утеряны. Закрытые порты часто оказываются еще большей проблемой. Обычно они в ответ возвращают ICMP ошибку о недостижимости порта. Но в отличии от RST пакетов отсылаемых закрытыми TCP портами в ответ на SYN или сканирование с установкой соединения, многие хосты ограничивают лимит ICMP сообщений о недостижимости порта по умолчанию. Linux и Solaris особенно строги в этом плане. Например, ядро Linux 2.4.20 огранивает количество таких сообщений до одного в секунду (в net/ipv4/icmp.c).

Nmap обнаруживает такого рода ограничения и соответственно сокращает количество запросов, чтобы не забивать сеть бесполезными пакетами, которые все равно будут отброшены целевой машиной. К сожалению, при ограничении в стиле Linux (один пакет в секунду) сканирование 65,536 портов займет более 18 часов. К способам увеличения скорости UDP сканирования относятся: параллельное сканирование нескольких хостов, сканирование в первую очередь только наиболее популярных портов, сканирование из-за брандмауэра и использование --host-timeoutдял пропуска медленных хостов.

-sN; -sF; -sX (TCP NULL, FIN и Xmas сканирования)

Эти три типа сканирования используют (другие типы сканирования доступны с использованием опции --scanflags описанной в другой секции) незаметную лазейку в TCP RFC, чтобы разделять порты наоткрытые и закрытые. На странице 65 RFC 793 говорится, что “если порт назначения ЗАКРЫТ .... входящий сегмент не содержащий RST повлечет за собой отправку RST в ответ.” На следующей странице, где обсуждается отправка пакетов без установленных битов SYN, RST или ACK, утверждается что: “вы врядли с этим столкнетесь, но если столкнетесь, то сбросьте сегменты и вернитесь к исходному состоянию.”

Когда сканируется система отвечающая требованиям RFC, любой пакет, не содержащий установленного бита SYN, RST или ACK, повлечет за собой отправку RST в ответ в случае, если порт закрыт, или не повлечет никакого ответа, если порт открыт. Т.к. ни один из этих битов не установлен, то любая комбинация трех оставшихся (FIN, PSH и URG) будет являться правильной. Nmap использует это в трех типах сканирования:

Null сканирование (-sN)- не устанавливаются никакие биты (Флагов в TCP заголовке 0)

FIN сканирование (-sF)- устанавливается только TCP FIN бит.

Xmas сканирование (-sX) - устанавливаются FIN, PSH и URG флаги.

Эти три типа сканирования работают по одной схеме, различия только в TCP флагах установленных в пакетах запросов. Если в ответ приходит RST пакет, то порт считается закрытым, отсутствие ответа означает, что порт открыт|фильтруется. Порт помечается как фильтруется, если в ответ приходит ICMP ошибка о недостижимости (тип 3, код 1, 2, 3, 9, 10 или 13).

Ключевой особенностью этих типов сканирования является их способность незаметно обойти некоторые не учитывающие состояние (non-stateful) брандмауэры и роутеры с функцией пакетной фильтрации. Еще одним преимуществом является то, что они даже чуть более незаметны, чем SYN сканирование. Все же не надо на это полагаться - большинство современных IDS могут быть сконфигурированы на их обнаружение. Большим недостатком является то, что не все системы следуют RFC 793 дословно. Некоторые системы посылают RST ответы на запросы не зависимо от того, открыт порт или закрыт. Это приводит к тому, что все порты помечаются как закрытые. Основными системами ведущими себя подобным образом являются MicrosoftWindows, многие устройства Cisco, BSDI и IBM OS/400. Хотя такое сканирование применимо к большинству систем, основанных на Unix. Еще одним недостатком этих видов сканирования является их неспособность разделять порты на открытые и фильтруемые, т.к. порт помечается как открыт|фильтруется.

-sA (TCP ACK сканирование)

Этот тип сканирования сильно отличается от всех других тем, что он не способен определить открый порт open (или даже открытый|фильтруемый). Он используются для выявления правил брандмауэров, определения учитывают ли он состояние или нет, а также для определения фильтруемых ими портов.

Пакет запроса при таком типе сканирования содержит установленным только ACK флаг (если не используется --scanflags). При сканировании нефильтруемых систем, открытые и закрытые порты оба будут возвращать в ответ RST пакет. Nmap помечает их как не фильтруемые, имея ввиду, что они достижимы для ACK пакетов, но неизвестно открыты они или закрыты. Порты, которые не отвечают или посылают в ответ ICMP сообщение об ошибке (тип 3, код 1, 2, 3, 9, 10 или 13), помечаются как фильтруемые.

-sW (TCP Window сканирование)

Этот тип сканирования практически то же самое, что и ACK сканирование, за исключением того, что он использует особенности реализации различных систем для разделения портов на открытые и закрытые, вместо того, чтобы всегда при получении RST пакета выводить не фильтруется. Это осуществляется путем анализа TCP Window поля полученного в ответ RST пакета. В некоторых системах открытые порты используют положительное значение этого поля (даже в RST пакетах), а закрытые - нулевое. Поэтому вместо того, что все время при получении RST пакета в ответ помечать порты как не фильтруемые, при Window сканировании порты помечаются как открытые или закрытые, если значение поля TCP Window положительно или равно нулю соответственно.

Этот тип сканирования основывается на особенностях реализации меньшинства систем в Интернете, поэтому является не таким надёжным. В общем случае в системах, не

имеющих таких особенностей, все порты будут помечаться как закрытые. Конечно, это возможно, что у машины действительно нет открытых портов. Если большинство просканированных портов закрыты, и лишь несколько распространненых портов (таких как 22, 25, 53) фильтруются, то скорее всего результатам сканирования можно доверять. Иногда, системы будут вести себя прямо противоположным образом. Если в результате сканирования будет найдено 1000 открытых портов и 3 закрытых или фильтруемых, то как раз эти 3 могут оказаться действительно открытыми.

-sM (TCP сканирование Мэймона (Maimon))

Этот тип сканирования носит имя своего первооткрывателя, УриелаМэймона (UrielMaimon). Он описал эту технику в журнале *Phrack*Magazine, выпуск #49 (Ноябрь 1996). Версия Nmap с поддержкой этого типа сканирования была выпущена через два номера. Техника практически такая же как и при NULL, FIN и Xmas сканированиях, только в качестве запросов используются запросы FIN/ACK. Согласно RFC 793 (TCP), в ответ на такой запрос должен быть сгенерирован RST пакет, если порт открыт или закрыт. Тем не менее, Уриел заметил, что многие BSD системы просто отбрасывают пакет, если порт открыт.

--scanflags (Заказное TCP сканирование)

С помощью опции --scanflagsможно разработать свой тип сканирования путем задания специфичных TCP флагов. Аргументом опции может быть числовое значение, например, 9 (PSH и FIN флаги), но использование символьных имен намного проще. Можно использовать любые комбинации URG, ACK, PSH, RST, SYN и FIN. Например, опцией --scanflags URGACKPSHRSTSYNFIN будут установлены все флаги, хотя это и не очень полезно для сканирования. Порядок задания флагов не имеет значения.

В добавлении к заданию желаемых флагов, можно также задать тип TCP сканирования (например, -sA или -sF). Это укажет Nmap на то, как необходимо интерпретировать ответы. Например, при SYN сканировании отсутствие ответа указывает на фильтруемый порт, тогда как при FIN сканировании - на открытый|фильтруемый.Nmap будет осуществлять заданный тип сканирования, но используя указанные вами TCP флаги вместо стандартных. Еслитип сканирования не был указан, то по умолчанию будет использоваться SYN.

-sO (Сканирование IP протокола)

Сканирование такого типа позволяет определить, какие IP протоколы (TCP, ICMP, IGMP и т.д.) поддерживаются целевыми машинами. Технически такое сканирование не является разновидностью сканирования портов, т.к. при нем циклически перебираются номера IP протоколов вместо номеров TCP или UDP портов. Хотя здесь все же используется опция -p для выбора номеров протоколов для сканирования, результаты выдаются в формате таблицы портов, и даже используется тот же механизм сканирования, что и при различных вариантах сканирования портов. Поэтому он достаточно близок к сканированию портов и описывается здесь.

Способ работы этого типа сканирования очень похож на реализованный в UDP сканировании. Вместо того чтобы изменять в UDP пакете поле, содержащее номер порта, отсылаются заголовки IP пакета, и изменяется 8 битное поле IP протокола. Заголовки обычно пустые, не содержащие никаких данных и даже правильного заголовка для требуемого протокола. Исключениями являются TCP, UDP и ICMP. Включение правильного заголовка для этих протоколов необходимо, т.к. в обратном случае некоторые системы не будут их отсылать, да и у Nmap есть все необходимые функции для их создания. Вместо того чтобы ожидать в ответ ICMP сообщение о недостижимости порта, этот тип сканирования ожидает ICMP сообщение о недостижимости *протокола*. Если Nmap получает любой ответ по любому протоколу, то протокол помечается как открытый. ICMP ошибка о недостижимости протокола (тип 3, код 2) помечает протокол как закрытый. Другие ICMP ошибки недостижимости (тип 3, код 1, 3, 9, 10 или 13) помечают протокол как фильтруемый (в то же время они показывают, что протокол ICMP открыт). Если не приходит никакого ответа после нескольких запросов, то протокол помечается как открыт|фильтруется

3. Краткие сведения о IDS Snort

Snort - это сетевая IDS, способная выполнять в режиме реального времени анализ трафика, передаваемого по контролируемому интерфейсу, с целью обнаружения попыток взлома или попыток поиска уязвимостей (таких, как переполнение буфера, сканирование портов, CGI-атаки, идентификация операционной системы, идентификация версий используемых сетевых сервисов и др.). Гибкость и удобство Snort основываются на трех основных качествах:

1. язык правил, используемый для описания свойств подозрительного и потенциально опасного трафика;
2. механизм оповещения об обнаружении атаки;
3.модульная архитектура кода, анализирующего трафик, основанная на концепции подключаемых модулей.

Следует отметить, что процедуры, декодирующие сетевой трафик, работают, начиная со 2-го уровня модели ISO/OSI. В настоящее время Snort поддерживает декодирование для интерфейсов Ethernet, SLIP и PPP.

Рассмотрим самый важный для нас компонент - язык правил. Правила задаются в конфигурационных файлахSnort с расширением .rules. Их синтаксис довольно прост:

ACTION PROTO SOU_IP_ADDR PORT1 DIRECTION DES_IP_ADDR PORT2 [(OPTIONS)], где

ACTION– действие,может принимать 3 значения: pass, log и alert.Директива pass указывает Snort на игнорирование пакет. Директива log определяет, что пакет должен быть передан процедуре журналирования, выбранной пользователем, для последующей записи в файл журнала. Наконец, директива alert генерирует уведомление об обнаружении пакета, удовлетворяющего правилу - опять же определенным пользователем способом - и потом уже передает пакет процедуре журналирования для последующего анализа.

Можно также использовать еще две директивы: activate и dynamic. Они позволяют для некоторого множества пакетов из одного правила вызывать другое. Например, может потребоваться при обнаружении пакета с явными признаками атаки на переполнение буфера осуществить генерацию уведомления об атаке и записать в файл журнала несколько последующих пакетов для дальнейшего их анализа. Такая функциональность как раз и достигается совместным использованием директив activate и dynamic.

PROTO– протокол, в котором осуществляется перехват. Например, tcp, icmp, udp, …

SOU_IP_ADDR, DES_IP_ADDR –ip-адрес отправителя и получателя. Snort не имеет механизма для разрешения имен (и вряд ли он появится в дальнейшем - по соображениям производительности), поэтому для задания хостов необходимо использовать их IP-адреса. Ключевое слово any позволяет задать все возможные адреса, для подсетей указываются CIDR-блоки.Символ ! инвертирует условие, т.е. !192.168.1.0/24 означает любой не принадлежащий подсети 192.168.1.0/24 IP-адрес. Кроме того, можно задавать списки адресов, перечисляя их через запятую и заключая в квадратные скобки: [192.168.2.0/24,192.169.3.54/32]. Также в конфигурационном файле Snort (обычно им является snort.conf) можно задать символическое обозначение некоторым SIDR'ам. Например, строка ipvarHOME_NET 192.168.137.0/24 позволяет использовать литеральную константу HOME_NET для обозначения сегмента 192.168.137.1 - 192.168.137.254 сети при задании правил.

PORT– порт.Задание номеров портов осуществляется точно также, как и в Linux-утилите ipchains. То есть кроме единственного номера порта можно задать диапазон портов через двоеточие, например, 6000:6010 - порты с 6000 по 6010 включительно, :1024 - порты с 1 по 1024, 1024: - порты с 1024 по 65536. Как и в случае IP-адресов, символ ! инвертирует условие, а ключевое слово any обозначает все порты.

DIRECTION- направление движения пакета:-> (одностороннее) - правило будет применяться только к пакетам, идущим с IP_ADDR1 на IP_ADDR2;<> (двустороннее) - направление движения пакета роли не играет.

OPTIONS– опциидля анализа пакета. Заключаемые в круглые скобки параметры являются необязательной частью правила - и одновременно самой важной частью системы обнаружения вторжения. Параметры могут определять текст уведомляющего об угрозе сообщения, задавать дополнительные действия при срабатывании правила и дополнительные условия на соответствие анализируемых пакетов данному правилу.Параметры отделяются друг от друга точкой с запятой, а ключевое слово параметра отделяется от его аргумента двоеточием.

Рассмотрим несколько параметров, задающих дополнительные условия на соответствие правилу:

ttl- задает значение поля TTL в заголовке IP-пакета;

tos - задает значение поля TOS в заголовке IP-пакета;

id - задает значение поля номера фрагмента в заголовке IP-пакета;

ipopts - задает значение поля параметров IP-пакета;

fragbits - задает биты фрагментации IP-пакета;

dsize - задает условия на размер IP-пакета;

flags - задает условия на наличие или отсутствие определенных TCP-флагов;

seq - задает номер сегмента TCP-пакета в последовательности;

ack - задает значение поля подтверждения в TCP-пакете;

itype - задает значение поля типа ICMP-пакета;

icode - задает значение поля кода ICMP-пакета;

icmp_id - задает значение поля ICMP ECHO ID в ICMP-пакете;

icmp_seq - задает номер ICMP ECHO пакета в последовательности;

content - задает искомый шаблон в содержимом пакета, а не в заголовке (шаблон можно задавать как в текстовом виде, так и в шестнадцатеричном);

content-list - этот параметр аналогичен параметру content за исключением того, что список искомых шаблонов берется из заданного файла;

offset - работает совместно с опцией content для определения смещения в пакете, с которого будет производиться анализ содержимого;

depth - аналогичен параметру offset и определяет положение в пакете, до которого будет производиться анализ содержимого;

nocase - отключает чувствительность к регистру при анализе содержимого пакета;

rpc - этот параметр позволяет более точно задать характеристики программных или процедурных вызовов RPC-сервисов.

Как можно заметить, перечисленные параметры позволяют создавать правила для перехвата практически любых пакетов, которые как-то могут угрожать безопасности. А если учесть, что Snort может перехватывать пакеты на канальном уровне, то его применение особенно интересно на хостах, защищенных файрволом, так как отбрасываемые файрволом пакеты все равно будут находиться в поле зрения Snort.

Параметры, значения которых имеют смысл при соответствии анализируемого пакета всем условиям:

msg - содержит текст сообщения;

logto - задает альтернативный файл для записи в него содержимого пакета;

session - этот параметр позволяет включить очень интересную возможность Snort - извлечение пользовательских данных из TCP-сессии, например, для последующего анализа того, какие команды вводил пользователь во время telnet-сессии;

resp - если пакет соответствует правилу, то Snort выполнит одно из указанных

действий - например, закроет соединение, отправив TCP-RST-пакет одному из хостов.

react - блокирует заданные в правиле web-сайты, закрывая соединение с ними и/или отправляя заданное сообщение браузеру, с которого была предпринята попытка зайти на сайт.

Примеры задания правил:

logtcpanyany -> 192.168.1.0/24 6000:6010

Все пакеты, адресованные на обычно используемые системой XWindow порты хостов некоторой подсети, будут записываться в лог.

alerttcp !192.168.1.0/24 any -> 192.168.1.0/24 any (msg:"IDS004 - SCAN-NULL Scan";flags:0; seq:0; ack:0;)

Такое правило обнаруживает попытку так называемого NULL-сканирования портов.

alerttcp !192.168.1.45/32 any -> 192.168.1.45/32 80 (msg:"IIS-_vti_inf";flags:PA; content:"_vti_inf.html"; nocase;)

Адресованные web-серверу пакеты, содержащие в себе запрос к файлу _vti_inf.html, рассматриваются как попытка воспользоваться одной из уязвимостей InternetInformationServer, что вызовет при обнаружении таких пакетов генерацию сообщения об этом событии, а сам пакет запишется в лог-файл.

activatetcp !192.168.1.0/24 any -> 192.168.1.0/24 143 (flags: PA; content: "|E8C0FFFFFF|\bin|"; activates: 1; msg: "IMAP buffer overflow!";) dynamic tcp !192.168.1.0/24 any -> 192.168.1.0/24 143 (activated_by: 1; count: 50;)

Директива activate ничем не отличается от alert за исключением того, что в разделе опций правила activate всегда присутствует опция activates, предназначенная для вызова на исполнение другого правила. Вызвать можно только правило dynamic. Директива dynamic в свою очередь ничем не отличается от директивы log. Она также предназначена для записи пакетов в лог, но имеет при этом два дополнительных параметра: activated_by, которая ассоциирует правило dynamic с правилами activate, а также count, которая указывает для какого количества пакетов должно отработать правило, то есть сколько пакетов, следующих за перехваченным пакетом должны быть записаны в лог. Приведенное выше правило activate анализирует пакеты на предмет попытки реализации атаки на переполнение буфера и в случае обнаружения таковой вызывает правило dynamic для записи в лог-файл следующих 50 пакетов. Если атака была успешной, то, анализируя

впоследствии файл, можно установить, какой именно урон был нанесен. Также такое правило может использоваться для «охоты» за новыми эксплойтами.

Порядок выполнения работы:

1. Написать alert-правило для Snort, выводящее в лог сообщение «Vkontacteisfacebookornot?», когда пользователь заходит на сайт vkontakte.ru (сделать это с помощью опций contenturiconent и сравнить результат);
2. Написать alert-правило для Snort, выводящее в лог «ICMPdetected», при прохождении через данный хост любого icmp-пакета.
3. Провести icmp-сканирование сегмента /24 сети лаборатории с помощью Nmap;
4. С помощью запуска Snortв режиме сниффера выявить отличия между пакетами, генерируемыми утилитой pingОС WindowsXP или 7 и *nix. Сравнить их с пакетами, генерируемыми при icmp-сканировании Nmap.
5. На основании результатов пункта 2, написать alert-правило для Snort, которое выводит в лог сообщение «Nmapicmp-scandetected», когда происходит icmp-сканированиеNmap.
6. Просканировать утилитойNmap компьютер с целью выявления ОС.
7. Просканировать утилитойNmapкомпьютер с целью выявления поддерживаемых протоколов.
8. Провести SYN, FIN, XMAS, TCP, TCPNULLсканирования портов с помощью Nmap, записать результат с помощью запуска Snort в режиме сниффера.
9. Написать alert-правила для Snort, выводящее в лог сообщение о Nmap сканировании вида «XNmapscanning», где X – это тип сканирования.

Каждое правило должно быть проверено на практике, а в отчёте должны содержаться скриншоты применений этих правил.

Полученные знания и навыки

В ходе выполнения лабораторной работы будут получены следующие основные навыки и знания:

- Углубленные знания о TCP/IP протоколе и возможных уязвимостях, связанных с работой с данным протоколом.
- Основные навыки работы со свободной утилитой Nmap:
  - Различные методы сканирования, такие как UDP, TCP (connect), TCP SYN (полуоткрытое), FTP proxy (прорыв через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN- и NULL-сканирование и др.
  - Определение состояния объектов сканируемой сети (портов и соответствующих им служб).
- Основные навыки работы со свободной сетевой системой предотвращения вторжений Snort:
  - Протоколирование необходимых сведений, анализ и поиск по содержимому сети с помощью alert-правил.

Все знания и навыки, полученные в ходе выполнения лабораторной работы, являются необходимыми для проведения аудита безопасности и пентеста ИС.

Контрольные вопросы:

1. Чем отличается IDSот IPS?
2. Какие значения может принимать ACTION в правилах Snort?
3. Что такое SIDR?
4. Что такое сетевое сканирование целевой системы?
5. Может ли Snortфильтровать пакеты?
6. Чем отличается SYNсканирование от FIN сканирования?
7. Зачем нужна опция sid в правилахSnort и какие она должна принимать значения для пользовательских правил?
8. Какой(ие) тип сканирования, поддерживаемый Nmap,может применяться для определения наличия на целевом компьютере файрволла?
9. Разберитеправило

   alerttcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (flow:to_server, established; content:"/hsx.cgi"; http_uri; content:"../../"; content:"%00"; distance:1; reference:cve,2001-0253; reference:nessus,10602; classtype:web-application-attack; sid:803; rev:17;).

   Длядетектированиякакогоклассауязвимостейономожетприменяться, и эксплойт на какую конкретную уязвимость оно может логировать?

10. На чём основана возможность определения с помощью сетевого сканирования версии ОС?

Занятие 4. Использование IDS Snort для обнаружения эксплойтов в сетевом трафике

Цель работы

Изучить основные способы детектирования эксплойтов с помощью IDS Snort, а также обучиться работе с Metasploit.

Теоретические сведения

Прежде чем перейти к освоению материала, введём некоторые определения:

Эксплойт (англ. exploit — использовать) — это общий термин для обозначения фрагмента программного кода (иногда просто последовательность символов) который, используя возможности предоставляемые ошибкой, отказом или уязвимостью, ведёт к повышению привилегий или отказу в обслуживании компьютерной системы.

Шелл-код (код оболочки, шелл-код (англ. shellcode)) — это двоичный исполняемый код, который обычно передаёт управление консоли, например '/bin/sh' Unix shell, command.com в MS-DOS и cmd.exe в операционных системах Microsoft Windows. Код оболочки может быть использован как полезная нагрузка эксплойта, обеспечивая взломщику доступ к командной оболочке (англ. shell) в компьютерной системе.

Реверс-шелл - при эксплуатации удаленной уязвимости шелл-код может открывать заранее заданный порт TCP уязвимого компьютера, через который будет осуществляться дальнейший доступ к командной оболочке, такой код называется привязывающим к порту (англ. port binding shellcode). Если шелл-код осуществляет подключение к порту компьютера атакующего, что производится с целью обхода брандмауэра или NAT, то такой код называется обратной оболочкой (англ. reverse shell shellcode).

Уязвимость (англ. vulnerability) –обозначение недостатка в системе, используя который, можно нарушить её целостность и вызвать неправильную работу. Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ, скриптовых, а также SQL-инъекций. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты. Обычно уязвимость позволяет атакующему «обмануть» приложение — заставить его совершить действие, на которое у того не должно быть прав. Это делается путем внедрения каким-либо образом в программу данных или кода в такие места, что программа воспримет их как «свои». Некоторые уязвимости появляются из-за недостаточной проверки данных, вводимых пользователем, и позволяют вставить в интерпретируемый код произвольные команды (SQL-инъекция, XSS). Другие уязвимости появляются из-за более сложных проблем, таких как запись данных в буфер без проверки его границ (переполнение буфера).

Сейчас для взлома системы, в основном, применяют различные виды эксплойтов. Но наиболее часто используемыми являются сетевые эксплойты с нагрузкой в виде

реверс-шеллов. Они позволяют получить удалённое управление системой, в которой есть подходящая уязвимость. При этом часто для атаки системы используют автоматизированные средства. Самым популярным из них является Metasploit Framework.

Metasploit Framework (согласно описанию) - это законченная среда для написания, тестирования и использования кода эксплойтов. Эта среда обеспечивает надежную платформу для испытаний на проникновение, разработки шелкодов и исследования уязвимостей". Написан на Perl (с некоторыми частями на ассемблере, Python и C) – отсюда нет привязки к какой либо платформе – может работать в любой системе, где есть интерпретатор Perl`a (с оговоркой, см. дальше). На данный момент, пакет Metasploit Framework функционирует как на Linux так и на Windows, а так же на Mac. Скачать последнюю версию пакета для соответствующей ОС можно здесь: http://www.metasploit.com/ (Среда под Windows базируется на доработанном Cygwin, что удобно, т.к. это дает пользователю известную консоль. Однако, были некоторые проблемы с поддержкой Active Perl, поэтому поддерживается только Cygwin Perl.)

Основное предназначение этого средства в упрощении работы пентестера по проверке системы на уязвимости. Metasploit содержит достаточно большую базу эксплойтов и шеллкодов. Он поставляется с 3-мя рабочими окружениями: msfconsole, msfcli и msfweb. Основным и наиболее предпочтительным из трех перечисленных вариантов является первый - msfconsole. Это окружение представляет собой эффективный интерфейс командной строки со своим собственным набором команд и системным окружением.

Перед запуском Metasploit полезно было бы понять, что делают хотя бы некоторые его команды:

1. **search <keyword>**: запустив команду search без указания ключевых слов, мы получим список всех доступных эксплоитов. Если значение <keyword> имеет имя определенного сплоита, то этой командой мы ищем такой в базе данных системы.

2. **show exploits**: указав команду show exploits, мы получим список всех доступных на данный момент эксплоитов под различные платформы и приложения, включая Windows, Linux, IIS, Apache и так далее. Это поможет вам понять работу фреймворка **Metasploit** и почувствовать его гибкость и эффективность.

3. **show payloads**: аналогично предыдущим командам show, показывает доступные в системе payload'ы. Запускаем команду show payloads и изучаем получившийся список.

4. **show options**: набрав в командной строке show options, вы увидите опции, которые вы можете использовать. Каждый эксплойт или payload имеет свой собственный набор опций, который вы можете использовать при работе с ними.

5. **info <type> <name>**: если вам нужна конкретная и полная информация о каком-либо эксплойте или payload'е, вы можете применить команду info. Скажем, вам нужно подробное описание payload'a winbind. Тогда мы набираем в командной

строке info payload winbind и внимательно читаем справочную информацию по нему.

6. **use <exploit_name>**: команда говорит фреймворку **Metasploit** запустить эксплойт с указанным конкретным именем.

7. **set RHOST <hostname_or_ip>**: указываем этой командой **Metasploit** определенный хост в сети для его изучения. Хост можно задать как по его имени, так и по IP-адресу.

8. **set RPORT <host_port>**: задаем для **Metasploit** порт удаленной машины, по которому фреймворк должен подключиться к указанному хосту.

9. **set payload <generic/shell_bind_tcp>**: команда указывает имя payload'a, который будет использоваться.

10. **set LPORT <local_port>**: задаем номер порта для payload'a на сервере, на котором был выполнен эксплойт. Это важно, так как номер этого порта открыт именно на сервере (он не может быть использован никакими другими службами этого сервера и не резервируется для административных нужд). Советую назначать такой номер из набора четырех случайных цифр, порядок которых начинается с 1024. Также стоит упомянуть, что Вам необходимо менять номер порта каждый раз, когда вы успешно запустите эксплойт на удаленной машине.

11. **exploit**: запущенный на данный момент эксплойт. Есть другая версия этой команды - rexploit, которая перезагружает код запущенного эксплойта и запускает его вновь. Эти две команды помогают вам работать с эксплойтами с минимальными усилиями, без перезапуска консоли.

12. **help**: команда help выдаст полный перечень всех доступных команд системы.

Теперь перейдём к практической части описания: воспользуемся уязвимостью IE 6.0 (ms10_00 aurora) для загрузки реверс-шелла. Компьютер-жертва имеет ip 192.168.2.21, а компьютер «атакующего» ip 192.168.2.20.

Процесс «заражения» происходит по следующей схеме (рисунок 1): пользователь заходит на страницу A (рисунок 5) сайта-приманки, где переходит по безобидной ссылке, желая попасть на некую страницу B. Но перед тем как попасть на желаемую страницу, пользователь перенаправляется на зараженную страницу C, где с небольшой задержкой отрабатывается вредоносный код. И только после этого пользователь попадает на страницу B. При этом пользователь не замечает заражения, так как страница C визуально не отображается. Более того, временная задержка, связанная с обработкой страницы C, минимальна и должна составлять доли секунды (хотя может и больше при очень медленном подключении к сети Интернет). На рисунке путь пользователя к сайту показан синей стрелкой (№1), нелегально передающийся вредоносный код - красной (№2), а информация, которую пользователь действительно хотел получить - зеленой (№3).

В нашей же схеме для простоты не будет страницы B, а эксплойт будет грузиться сразу при открытии соответствующей страницы в браузере.

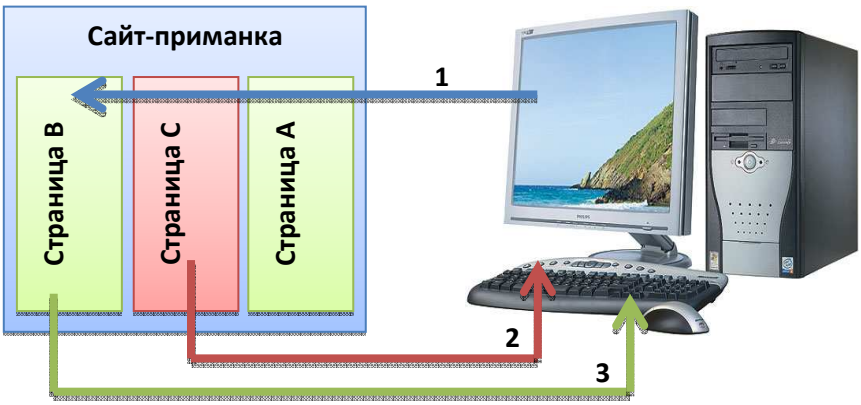


Рисунок 1. Схема заражения компьютера-жертвы

1. Загрузим Metasploit console и выберем соответствующий эксплойт (рисунок 2).

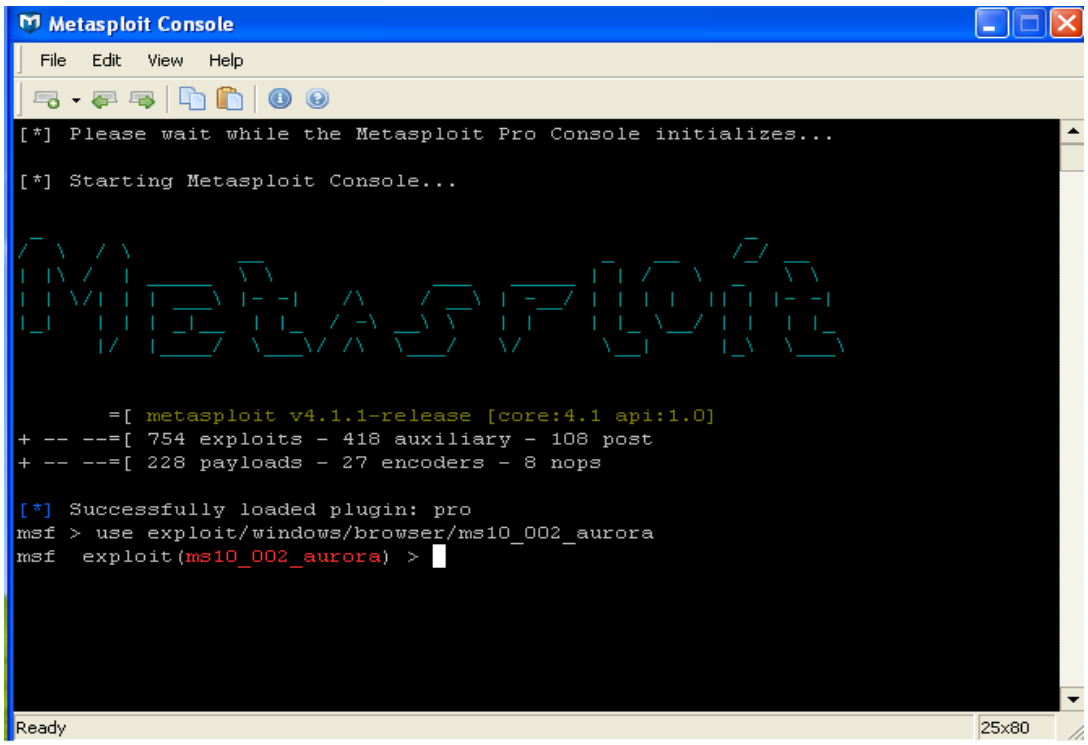


Рисунок 2. Внешний вид консоли Metasplot’a

2. У каждого эксплойта есть параметры, которые нужно установить перед его непосредственным использованием. В нашем случае это SRVHOST (ip адрес хоста, на котором будет располагаться сервер для управления шеллом) и URIPATH («вредоносная» ссылка, по которой нужно будет перейти пользователю).

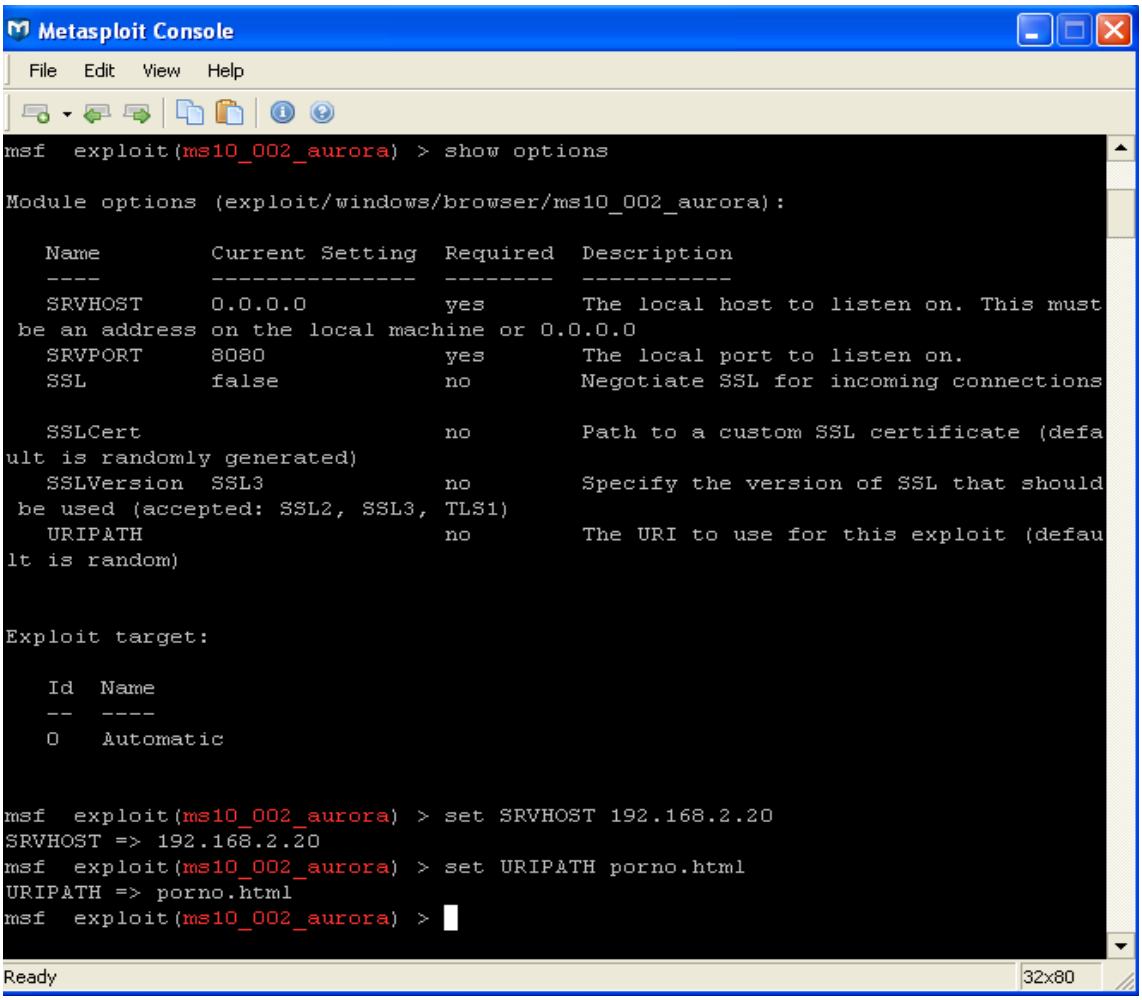


Рисунок 3. Установка параметров эксплойта

3. Дальше нам нужно выбрать шеллкод (рисунок 4), который будет загружаться на компьютер-жертву. Выберем реверс-шелл. У каждого шеллкода также несколько параметров настройки: LHOST (адрес, которому будет предоставлена возможность управления реверс-шеллом), LPORT и EXITFUNC (способ завершения работы).

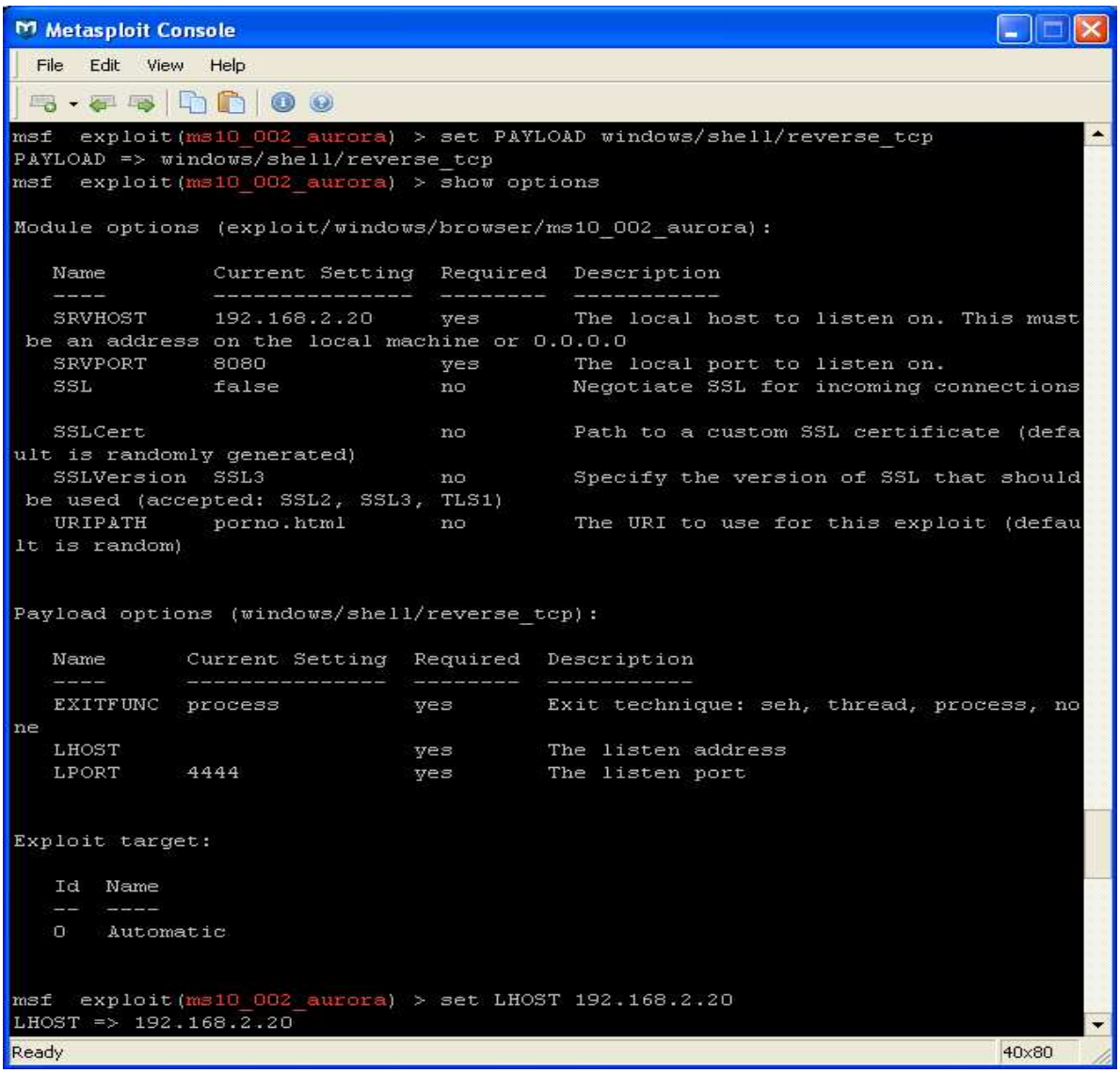


Рисунок 4. Выбор эксплойта и настройка его параметров

4. После этого настройка эксплойта и шелкода является завершённой и их можно использовать (рисунок 5).

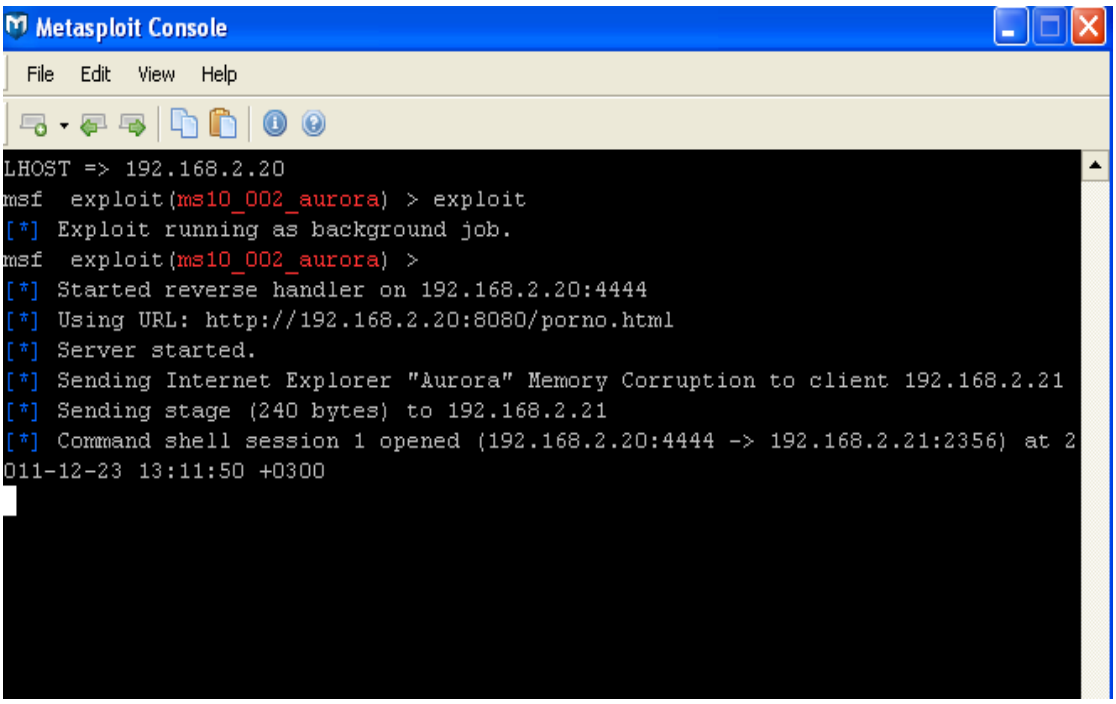


Рисунок 5. Запуск веб-сервера

5. Теперь осталось только на компьютере-жертве перейти на вредоносную ссылку. После чего в консоле будут показаны шаги загрузки эксплойта (рисунок 5).
6. После успешной загрузки нужно просмотреть список сессий и выбрать нужную нам (рисунок 6). После чего мы получим доступ к cmd.exe жертвы.

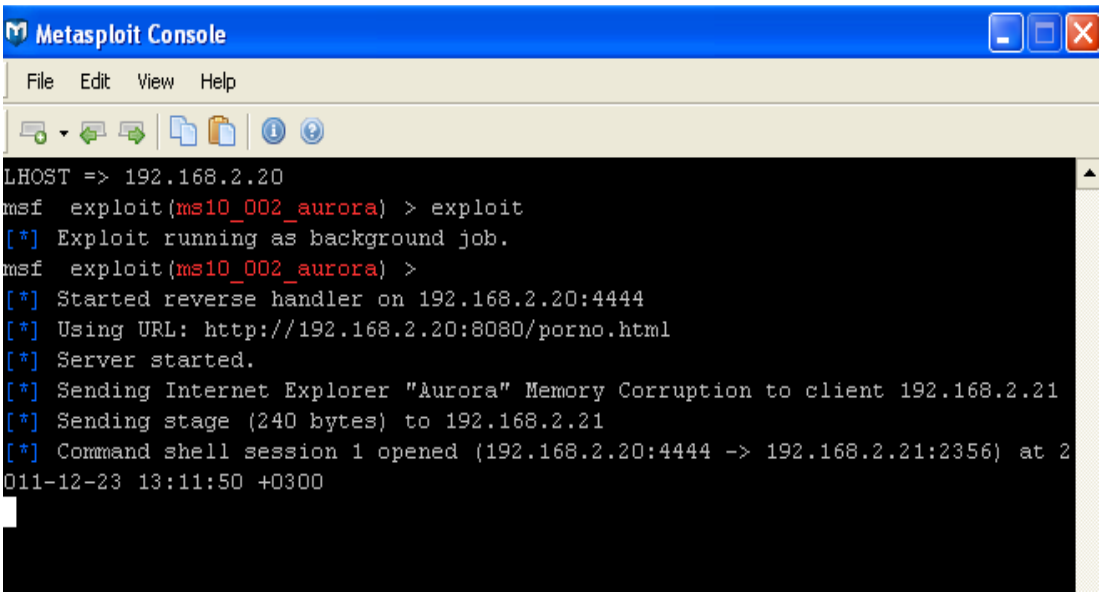


Рисунок 6. Управление сессиями Metasploit’а

Полученные знания и навыки

В ходе выполнения лабораторной работы будут получены следующие основные навыки и знания:

- Основные навыки работы со средой Metasploit Framework:
  - Настройка и запуск эксплойта из базы Metasploit Framework.
  - Использование эксплойта для выполнения действий, запрещенных правами доступа.
- Основные навыки работы со свободной сетевой системой предотвращения вторжений Snort:
  - Протоколирование необходимых сведений, анализ и поиск по содержимому сети с помощью alert-правил.
  - Определение «сетевой атаки» по содержимому TCP-пакетов.

Все знания и навыки, полученные в ходе выполнения лабораторной работы, являются необходимыми для проведения аудита безопасности и пентеста ИС.

Порядок выполнения работы:

1. Настройте и запустите эксплойт с помощью metasploit на 192.168.2.20.
2. Откройте «вредоносную страницу» на 192.168.2.21, проверьте работу реверс-шелла
3. Запишите вредоносный трафик с помощью IDS Snort
4. Напишите правило Snort для детектирования эксплойта ms10_002_aurora
5. Откройте «вредоносную страницу» на 192.168.2.21 и просмотрите результат работы Snort

Вопросы к экзамену

1. Основные понятия, термины и определения в области информационной безопасности.
2. Классификация угроз безопасности информации.
3. Структура системы защиты информации.
4. Основные направления защиты конфиденциальной информации.
5. Законодательная и нормативная база правового регулирования вопросов защиты информации ограниченного доступа.
6. Руководящие документы по защите информации от несанкционированного доступа.
7. В чем состоит принципиальное отличие криптографических и криптоаналитических методов?
8. Что называют криптографическим ключом?
9. Поясните сущность и сравните между собой криптографический алгоритм, криптографический протокол и криптографическую систему зашиты информации.
10. Что подразумевают под аутентификацией информации?
11. Перечислите криптографические функции?
12. В чем состоит принципиальное отличие симметричных и несимметричных систем шифрования информации?
13. Перечислите режимы защиты информации по ГОСТ 28147-89. В чем состоит существенное отличие методов защиты информации по ГОСТ 28147-89 от методов согласно стандарта шифрования DES?
14. Использование электронной цифровой подписи в ИСПДн.
15. Какой недостаток цифровых подписей с использованием симметричных шифросистем?
16. Для чего цифровой подписи нужно хеширование?
17. Понятие бесключевой хеш-функции. Свойство односторонности.
18. Понятие систем установки и управления ключами.
19. Понятие систем открытого распределения ключей.
20. Понятие сертификата открытого ключа.
21. Суть стандарта ISO X.509.
22. Задачи центра сертификации.
23. Понятие иерархии Центров сертификации.
24. Типы средств защиты информации от НСД. Сравнительные характеристики СЗИ от НСД («Криптон»,«Secret Net», «Застава», «Верба», «ViPNet» и т. д.).
25. Техническое обслуживание, гарантийный и постгарантийный ремонт основных технических средств и систем.

1. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции
   наследованию
   полиморфизму

2. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
   запрет на чтение каких-либо файлов, кроме конфигурационных
   запрет на изменение каких-либо файлов, кроме конфигурационных
   запрет на установление сетевых соединений

3. Необходимость объектно-ориентированного подхода к информационной безопасности является следствием того, что:
   это простой способ придать информационной безопасности научный вид
   объектно-ориентированный подход - универсальное средство борьбы со сложностью современных информационных систем
   в информационной безопасности с самого начала фигурируют понятия объекта и субъекта

4. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   меры обеспечения целостности
   административные меры
   меры административного воздействия

5. Контейнеры в компонентных объектных средах предоставляют:
   общий контекст взаимодействия с другими компонентами и с окружением
   средства для сохранения компонентов
   механизмы транспортировки компонентов

6. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности

7. Melissa подвергает атаке на доступность:
   системы электронной коммерции
   геоинформационные системы
   системы электронной почты

8. Выберите вредоносную программу, которая открыла новый этап в развитии данной области:
   Melissa
   Bubble Boy
   ILOVEYOU

9. Самыми опасными источниками внутренних угроз являются:
   некомпетентные руководители
   обиженные сотрудники
   любопытные администраторы

10. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
    просчеты при администрировании информационных систем
    необходимость постоянной модификации информационных систем
    сложность современных информационных систем

11. Агрессивное потребление ресурсов является угрозой: доступности конфиденциальности целостности

12. . Melissa - это:
    бомба

вирус
червь

13. Для внедрения бомб чаще всего используются ошибки типа:
отсутствие проверок кодов возврата
переполнение буфера
нарушение целостности транзакций

14. Окно опасности появляется, когда:
становится известно о средствах использования уязвимости
появляется возможность использовать уязвимость
устанавливается новое П

15. Среди нижеперечисленного выделите троянские программы:
ILOVEYOU
Back Orifice
Netbus

16. Уголовный кодекс РФ не предусматривает наказания за:
создание, использование и распространение вредоносных программ
ведение личной корреспонденции на производственной технической базе
нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

17. В законопроекте "О совершенствовании информационной безопасности" (США, 2001 год) особое внимание обращено на: смягчение ограничений на экспорт криптосредств
разработку средств электронной аутентификации
создание инфраструктуры с открытыми ключами

18. Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:
средства выявления злоумышленной активности
средства обеспечения отказоустойчивости
средства контроля эффективности защиты информации

19. Уровень безопасности B, согласно "Оранжевой книге", характеризуется:
произвольным управлением доступом
принудительным управлением доступом
верифицируемой безопасностью

20. В число классов требований доверия безопасности "Общих критериев" входят:
разработка
оценка профиля защиты
сертификация

21. Согласно "Оранжевой книге", политика безопасности включает в себя следующие элементы:
периметр безопасности
метки безопасности
сертификаты безопасности

22. Согласно рекомендациям X.800, выделяются следующие сервисы безопасности:
управление квотами
управление доступом
экранирование

23. Уровень безопасности A, согласно "Оранжевой книге", характеризуется:
произвольным управлением доступом
принудительным управлением доступом
верифицируемой безопасностью

24. Согласно рекомендациям X.800, аутентификация может быть реализована на:
    сетевом уровне
    транспортном уровне
    прикладном уровне

25. В число целей политики безопасности верхнего уровня входят:
    решение сформировать или пересмотреть комплексную программу безопасности
    обеспечение базы для соблюдения законов и правил
    обеспечение конфиденциальности почтовых сообщений

26. В число целей программы безопасности верхнего уровня входят:
    управление рисками
    определение ответственных за информационные сервисы
    определение мер наказания за нарушения политики безопасности

27. В рамках программы безопасности нижнего уровня осуществляются:
    стратегическое планирование
    повседневное администрирование
    отслеживание слабых мест защиты

28. Политика безопасности строится на основе:
    общих представлений об ИС организации
    изучения политик родственных организаций
    анализа рисков

29. В число целей политики безопасности верхнего уровня входят:
    формулировка административных решений по важнейшим аспектам реализации программы безопасности
    выбор методов аутентификации пользователей
    обеспечение базы для соблюдения законов и правил

1. В качестве аутентификатора в сетевой среде могут использоваться:
   кардиограмма субъекта
   номер карточки пенсионного страхования
   результат работы генератора одноразовых паролей

2. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:
   перехвата
   воспроизведения
   атак на доступность

3. В число основных понятий ролевого управления доступом входит:
   роль
   исполнитель роли
   пользователь роли

4. При использовании версии сервера аутентификации Kerberos, описанной в курсе:
   шифрование не применяется-
   применяется симметричное шифрование
   применяется асимметричное шифрование

5. При использовании описанного в курсе подхода к разграничению доступа в объектной среде наследование: учитывается всегда
   учитывается иногда
   не учитывается

6. В качестве аутентификатора в сетевой среде могут использоваться:
   год рождения субъекта
   фамилия субъекта
   секретный криптографический ключ

7. Ролевое управление доступом использует следующее средство объектно-ориентированного подхода:
   инкапсуляция
   наследование
   полиморфизм

8. Сервер аутентификации Kerberos:
   не защищает от атак на доступность
   частично защищает от атак на доступность
   полностью защищает от атак на доступность

9. В число основных понятий ролевого управления доступом входит:
   объект
   субъект
   метод

10. При использовании описанного в курсе подхода к разграничению доступа в объектной среде разграничивается доступ к:
    интерфейсам объектов
    методам объектов (с учетом значений фактических параметров вызова)
    классам объектов

1. В качестве аутентификатора в сетевой среде могут использоваться:
   кардиограмма субъекта
   номер карточки пенсионного страхования
   результат работы генератора одноразовых паролей

2. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:
   перехвата
   воспроизведения
   атак на доступность

3. В число основных понятий ролевого управления доступом входит:
   роль
   исполнитель роли
   пользователь роли

4. При использовании версии сервера аутентификации Kerberos, описанной в курсе:
   шифрование не применяется-
   применяется симметричное шифрование
   применяется асимметричное шифрование

5. При использовании описанного в курсе подхода к разграничению доступа в объектной среде наследование: учитывается всегда
   учитывается иногда
   не учитывается

6. В качестве аутентификатора в сетевой среде могут использоваться:
   год рождения субъекта
   фамилия субъекта
   секретный криптографический ключ

7. Ролевое управление доступом использует следующее средство объектно-ориентированного подхода:
   инкапсуляция
   наследование
   полиморфизм

8. Сервер аутентификации Kerberos:
   не защищает от атак на доступность
   частично защищает от атак на доступность
   полностью защищает от атак на доступность

9. В число основных понятий ролевого управления доступом входит:
   объект
   субъект
   метод

10. При использовании описанного в курсе подхода к разграничению доступа в объектной среде разграничивается доступ к:
    интерфейсам объектов
    методам объектов (с учетом значений фактических параметров вызова)
    классам объектов