ГБПОУ СПТ им. Б.Г.Музрукова

МДК.03.01. Технические методы и средства , технологии защиты информации
Раздел 4. Организационные основы инженерно-технической защиты информации

Лекция 36

Организация инженерно-технической защиты информации на предприятиях (в организациях, учреждениях)

Разработчик: Столяров И.В.,
преподаватель ГБПОУ СПТ им. Б.Г.Музрукова

г. Саров
2017

Предприятия (фирмы, организации, учреждения) — наиболее многочисленные структуры, в которых создается наибольший объем (количество) информации, содержащей государственную и конфиденциальную тайну. В них проводится конкретная и разнообразная работа по защите информации.

Независимо от формы собственности организация для проведения работ с информацией, содержащей государственную тайну, должна получить лицензию, т. е. выполнить предварительно в полном объеме требования по защите информации, предусмотренные соответствующими документами. После получения лицензии организация становится элементом государственной системы защиты информации, содержащей государственную тайну.

Для защиты информации, содержащей государственную тайну, на предприятии (в учреждении, организации) создаются в зависимости от объема работ по защите информации структурные подразделения или штатные специалисты, которые могут входить в состав одного из подразделений или службы безопасности. Их основными функции являются следующие:

- планирование работ по защите информации на предприятии (в учреждении, организации), разработка предложений по совершенствованию его системы защиты информации;
- определение демаскирующих признаков предприятия (учреждения, организации) и выпускаемой продукции;
- участие в подготовке предприятия (учреждения, организации) к аттестованию на право проведения работ с использованием сведений, отнесенных к государственной тайне;
- организация разработки нормативно-методических документов, разработка проектов распорядительных документов по вопросам организации защиты информации на предприятии;
- участие в согласовании ТЗ (ТТЗ) на проведение работ, содержащих государственную тайну, в разработке требований по защите информации при проведении исследований, разработке (модернизации), производстве и эксплуатации образцов продукции, при проектировании, строительстве и эксплуатации объектов (учреждения, организации);
- проведение периодического контроля эффективности мер защиты информации на предприятии (в учреждении, организации), участие в расследовании нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению нарушений;
- организация проведения занятий с руководящим составом и специалистами предприятия (учреждения, организации) по вопросам защиты информации.

Для защиты информации, составляющей коммерческую тайну, ее владелец создает собственную систему защиты информации. Законодательно структура такой системы не закреплена. Она определяется многими факторами: видом деятельности, уровнем конфиденциальности информации и ее объемом, штатной численностью ее сотрудников, финансовым состоянием фирмы и др. Однако для любой фирмы однотипны объективные функции сил и средств обеспечения защиты информации. Их может выполнять как полноценная структура, включающее большое количество людей и технических средств, так и несколько человек для малой фирмы. В принципе, так же как в государственных структурах, каждый сотрудник фирмы должен в объеме должностных обязанностей обеспечивать защиту информации. Об этом он информируется при приеме на работу. Эти требования указываются, как правило, в договоре между работодателем и работником.

Наиболее полно вопросы организация системы безопасности фирмы рассмотрены в [2]. Система безопасности фирмы образует следующие основные элементы (должностные лица и органы):

- руководитель фирмы, курирующий вопросы безопасность информации;
- совет по безопасности фирмы;
- служба безопасности фирмы;
- подразделения фирмы, участвующие в обеспечении безопасности фирмы.

Руководство безопасностью возлагается, как правило, на руководителя фирмы и его заместителя по общим вопросам (1-го заместителя), которым непосредственно подчиняется служба безопасности.

Совет по безопасности фирмы представляет собой коллегиальный орган при руководителе фирмы, состав которого назначается им из числа квалифицированных и ответственных по вопросам информационной безопасности должностных лиц. Совет безопасности разрабатывает для руководителя предложения по основным вопросам обеспечения безопасности информации, в том числе: направлениям деятельности по обеспечению безопасности фирмы и ее подразделений, совершенствования системы безопасности, взаимодействия с органами власти, заказчиками, партнерами, конкурентами и потребителями продукции и др.

Структурные подразделения занимаются вопросами защиты информации, которую они создают или используют в своей деятельности. Содержание и количество информации меняются во времени, в зависимости от решаемых задач и этапов деятельности. Однако основные и побочные результаты деятельности содержат защищаемую информацию еще длительное время, равное времени ее старения.

Служба безопасности является основным структурным подразделением по обеспечению безопасности, в том числе информационной, на фирме. Основными ее задачами в части информационной безопасности являются:

- мониторинг угроз информации;
- организация работы по защите информации на фирме;
- управление доступом сотрудником, автотранспорта и посетителей на территорию и в помещения фирмы;
- обеспечение безопасности информации при проведении всех видов деятельности внутри и вне фирмы, в том числе при чрезвычайных ситуациях;
- охрана территории, зданий, помещений и других мест и конструкций с защищаемой информацией.

Кроме этих задач служба безопасности обеспечивает охрану материальных ценностей фирмы и безопасность руководителей, ведущих специалистов и сотрудников.

Для решения указанных задач в полном объеме в службе безопасности создаются отдельные подразделения, примерный состав которых приведен на рис. 25.1.

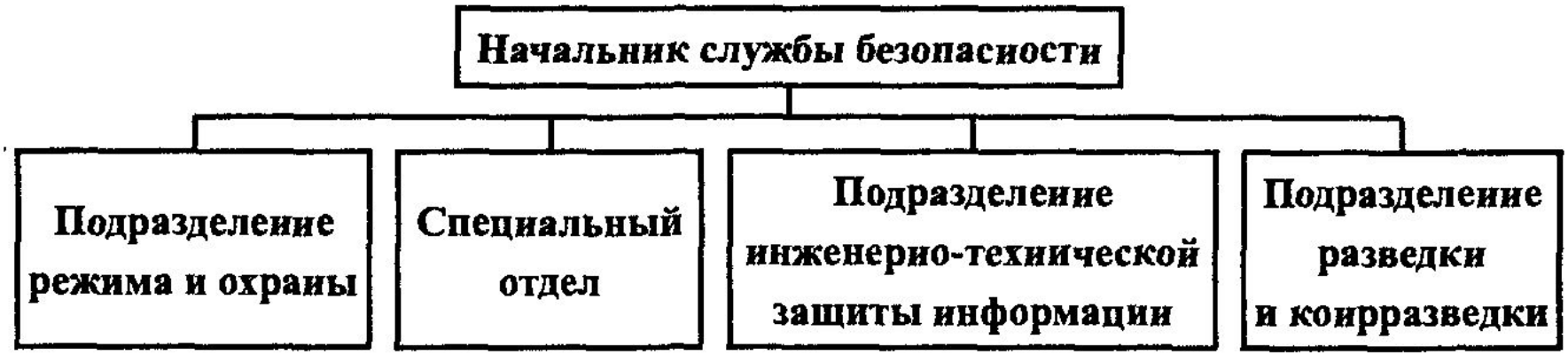

Рис. 25.1. Структура службы безопасности фирмы

Подразделение режима и охраны обеспечивает:

- организацию и контроль режима организации;
- охрану объектов организации и ее отдельных сотрудников, а также ценного груза при его перевозке за пределами организации.

В общем случае под режимом организации понимаются установленные законодательством, подзаконными актами и руководством организации условия работы в ней. В принципе для обеспечения эффективной деятельности любой организация в ней устанавливается определенный режим работы сотрудников. Если технологический процесс производства продукции непрерывен, то этот процесс должны обеспечивать сотрудники независимо от выходных, праздников, болезни и других обстоятельств. Например, нельзя временно, на праздники, потушить доменную печь, так как после этого нельзя восстановить ее работу без почти катастрофических последствий.

Однако обычно режим предполагает условия работы, направленные на обеспечение безопасности ценностей, в том числе информации. В этом смысле организацию с таким режимом называют **режимной**.

Ответственные сотрудники подразделения режима и охраны не только конкретизируют документы вышестоящих организация по режиму и разрабатывают внутри объектовые документы, но и контролируют выполнение их работниками организации. Например, сотрудники подразделения осматривают подозрительные предметы, которые могут вносить (ввозить) или выносить (вывозить) работники и посетители, контролируют способы переноса и хранения продукции с защищаемыми признаками, надежность закрытия и состояние печатей запасных дверей и ворот, порядок сдачи выделенных помещений под охрану и их вскрытия и др. Сотрудники подразделения режима и охраны занимаются также расследованием нарушений режима в организации.

Основу санкционированного доступа в контролируемые зоны составляет **пропускной режим**. Традиционно пропускной режим обеспечивается с помощью удостоверений и пропусков. Пропуска для сотрудников и посетителей могут быть постоянными, временными и разовыми, а также материальные для ввоза и вывоза материальных ценностей. Постоянные документы выдаются на несколько лет с последующей перерегистрацией или заменой, временные на несколько месяцев, разовые — на один день. Образцы удостоверений и пропусков разрабатываются службой безопасности и утверждаются руководством организации. Однако эти документы относятся к атрибутным идентификаторам со всеми присущими им недостатками. Их постепенно вытесняют более защищенные атрибутные идентификаторы (карты на различных принципах работы) и биометрические идентификаторы.

Для охраны объектов организации привлекаются в зависимости от их ведомственной принадлежности силы и средства подразделений охраны МО, МВД и коммерческих охранных структур, а также создаются собственные группы охраны. При использовании внешних сил охраны подразделение режима осуществляет контроль за выполнением ими своих функций. Группа охраны организации входит в состав ее подразделения режима и охраны и осуществляет охрану и контроль собственными силами.

Специальный отдел обеспечивает учет всех грифованных документов (входящей и исходящей корреспонденции, разрабатываемых и размножаемых в организации документов), циркулирующих в организации, ее централизованное хранение и санкционированной доступ к ней сотрудников организации. В специальном отделе учитывают также образцы продукции (веществ, макетов, узлов и др.), содержащие защищаемую информацию. Основанием для выдачи сотрудников документов и образцов продукции служат временные и разовые допуски, оформляемые руководителями структурных подразделений.

Защита информации с помощью инженерных конструкций и технических средств возлагается на **подразделение инженерно-технической защиты информации**. Оно занимается выявлением потенциальных угроз, разработкой мер по их предотвращению, инструментальным контролем уровней опасных сигналов и эксплуатацией технических средств защиты информации.

Любая организация, в том числе принадлежащая государству, нуждается для обеспечения эффективной деятельности в информации о партнерах и конкурентах. Для добывания этой информации в рамках как деловой разведки, так и промышленного шпионажа создается в организации **подразделение разведки** и **контрразведки**. Это подразделение обеспечивает:

- добывание данных и сведений и их аналитическую обработку с целью получения разведывательной информации о партнерах и конкурентах;
- прогнозирование угроз информации организации со стороны конкурентов и иных злоумышленников;
- разработка предложений по контрразведывательному обеспечению информационной безопасности.

Основная часть информации (по некоторым оценкам, до 95%) добывается из открытых источников, в особенности по вопросам, касающимся тенденций рынка, потенциальных конкурентов, надежности фирм, с которыми собирается сотрудничать организация и др. Однако информация об оригинальных схемотехнических, конструкторских и технологических решениях, реализация которых в продукции может обеспечить ее владельцам существенные преимущества перед конкурентами, закрывается и защищается.

Вопросы для самопроверки

1. Основные задачи государственной системы защиты информации от технической разведки.
2. Сущность категорий нарушений требований по защите информации.
3. Структура государственной защиты информации от технической разведки.
4. Задачи и структура Федеральной службы по техническому и экспортному контролю РФ (Государственной технической комиссии).
5. Задачи и структура органов по защите информации Федеральной службы безопасности России.
6. Задачи органов по обеспечению защиты информации ведомств.
7. Виды и органы лицензирования продукции, деятельности и услуг по защите информации.
8. Задачи и органы, обеспечивающие сертификацию средств по защите информации.
9. Задачи и структура по защите информации в организациях (учреждениях, на предприятиях).
10. Классификация документов нормативно-правовой базы по защите информации.
11. Назначение руководящих и нормативно-методических документов по защите информации.

Литература

1. *Гарсиа М.* Проектирование и оценка систем физической защиты. Пер. с англ. — М.: АСТ, 2002.
2. *Каторин Ю. Ф., Куренков Е. В., Лысов А. В., Остапенко А. Н.* Энциклопедия промышленного шпионажа. — СПб.: Полигон, 2000.
3. *Меньшаков Ю. К.* Защита информации от технических средств разведки. — М.: РГГУ, 2002.
4. *Петраков А. В., Дорошенко П. С., Савлуков Н. В.* Охрана и защита современного предприятия. — М.: Энергоатомиздат, 1999.
5. Специальная техника и информационная безопасность: Учебник. Т. 1 / Под ред. *В. И. Кирина.* — М.: Академия управления МВД России, 2000.
6. *Торокин А. А.* Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.
7. *Хорев А. А.* Способы и средства защиты информации. — М.: МО РФ, 1998.
8. *Хорев А. А.* Теоретические основы оценки возможностей технических средств разведки. — М.: МО РФ, 2000.