Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Тамбовский государственный технический университет»

Ю. Ю. ГРОМОВ, О. Г. ИВАНОВА, Ю. Ф. МАРТЕМЬЯНОВ и др.

МЕТОДЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

Рекомендовано Учёным советом университета в качестве
учебного пособия для студентов 3–4 курсов всех форм обучения
направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55

Тамбов
♦ Издательство ФГБОУ ВПО «ТГТУ» ♦
2013

УДК 004.056.5(075.8)
ББК з973я73
М54

Рецензенты:

Кандидат технических наук, профессор кафедры
«Информатика и информационные технологии» ФГБОУ ВПО
«ТГУ им. Г. Р. Державина»
И. А. Зауголков

Доктор технических наук, профессор кафедры «КРЭМС»
ФГБОУ ВПО «ТГТУ»
В. Н. Шамкин

Авторский коллектив:

Ю. Ю. Громов, О. Г. Иванова, Ю. Ф. Мартемьянов,
Ю. К. Букурако, В. Г. Однолько

М54 **Методы** организации защиты информации : учебное пособие для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55 / Ю. Ю. Громов и др. – Тамбов : Изд-во ФГБОУ ВПО «ТГТУ», 2013. – 80 с. – 100 экз. – ISBN 978-5-8265-1235-7.

Изложены цели и задачи организационной защиты информации, виды угроз информационной безопасности на объекте защиты, основные направления, принципы и условия организационной защиты информации. Описана организационная структура службы безопасности, освещены вопросы обеспечения безопасности информации при проведении совещаний, переговоров, работе с персоналом. Также рассмотрены вопросы организации охраны объектов и пропускного режима.

Предназначено для студентов 3–4 курсов всех форм обучения направлений подготовки 230400.55, 230701.51, 090300.65, 220100.55.

УДК 004.056.5(075.8)
ББК з973я73

ISBN 978-5-8265-1235-7

ПРЕДИСЛОВИЕ

В учебном пособии рассматриваются ключевые разделы курса «Методы организации защиты информации», направленные на развитие следующих компетенций:

– способность организовать эксплуатацию автоматизированной системы с учётом требований информационной безопасности (ПК-30);

– способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности (ПК-31);

– способность проводить анализ особенностей деятельности организации и использования в ней автоматизированных систем в целях определения информационно-технологических ресурсов, подлежащих защите (ПК-32);

– способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность её реализации (ПК-33);

– способность формировать комплекс мер (правила, процедуры, практические приёмы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной системы (ПК-34).

Организационная защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учётом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.

Среди основных направлений защиты информации наряду с организационной выделяют правовую и инженерно-техническую защиту информации. Однако организационной защите информации среди этих направлений отводится особое место. Организационная защита информации призвана посредством выбора конкретных сил и средств (включающие в себя правовые, инженерно-технические и инженерно-геологические) реализовать на практике спланированные руководством предприятия меры по защите информации. Эти меры принимаются в зависимости от конкретной обстановки на предприятии, связанной с наличием возможных угроз, воздействующих на защищаемую информацию и ведущих к её утечке.

Весь материал учебного пособия базируется только на открытых публикациях в Интернете и отечественной печати.

Авторы не претендуют на исчерпывающую полноту изложенного материала и заранее благодарны читателям, которые пришлют свои замечания и пожелания по адресу: runc@tstu.ru.

1. ВВЕДЕНИЕ В КУРС

1.1. ЦЕЛИ И ЗАДАЧИ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ, ЕЁ СВЯЗЬ С ПРАВОВОЙ И ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТОЙ ИНФОРМАЦИИ

Зарубежный опыт в области защиты интеллектуальной собственности и отечественный опыт в защите государственных секретов показывает, что эффективной может быть только комплексная защита, сочетающая в себе такие направления защиты, как: *правовое*, *организационное* и *инженерно-техническое*.

Правовое направление предусматривает формирование совокупности законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых являются обязательными в рамках сферы их деятельности в системе защиты информации.

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

По мнению специалистов, организационные мероприятия играют большую роль в создании надёжного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты.

Влияние этих аспектов практически невозможно избежать с помощью технических средств, программно-математических методов и физических мер.

К организационным мероприятиям можно отнести:

– мероприятия, осуществляемые при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений. Их цель – исключение возможности тайного проникновения на территорию и в помещения; обеспечение удобства контроля прохода и перемещения людей, проезда транспорта и других средств передвижения; создание отдельных производственных зон по типу конфиденциальности работ с самостоятельными системами доступа и т.п.;

– мероприятия, осуществляемые при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организация и поддержание надёжного пропускного режима и контроля посетителей;

– организация надёжной охраны помещений и территории;

– организация хранения и использования документов и носителей конфиденциальной информации, включая порядок учёта, выдачи, исполнения и возвращения;

– организация защиты информации: назначение ответственного за защиту информации в конкретных производственных коллективах, проведение систематического контроля за работой персонала с конфиденциальной информацией, порядок учёта, хранения и уничтожения документов и т.п.;

– организация регулярного обучения сотрудников.

Инженерно-техническое направление включает в себя программно-аппаратные средства защиты информации. К аппаратным средствам относятся механические, электромеханические, электронные, оптические, лазерные, радио- и радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для обеспечения безопасности и защиты информации.

Эти средства применяются для решения следующих задач:

– препятствия визуальному наблюдению и дистанционному подслушиванию;

– нейтрализации паразитных электромагнитных излучений и наводок (ПЭМИН);

– обнаружения технических средств подслушивания и магнитной записи, несанкционированно устанавливаемых или проносимых в организацию;

– защиты информации, передаваемой в средствах связи и системах автоматизированной обработки информации.

По своему предназначению аппаратные средства подразделяются на средства выявления и средства защиты (или существенного ослабления) несанкционированного доступа.

К классу защитной спецтехники относится огромное количество аппаратов, устройств и систем, которые условно можно разделить на несколько групп. Например, на такие как:

– приборы обнаружения и нейтрализации подслушивающих и звукозаписывающих устройств;

– средства защиты абонентской телефонной сети;

– средства защиты съёма информации из помещений;

– приборы для обнаружения лазерного и видеонаблюдения и др.

Многогранность сферы организационной защиты информации требует создания специальной службы безопасности, обеспечивающей и направляющей реализацию всех организационных мероприятий. Её штатная структура, численность и состав определяется реальными потребностями фирмы, степенью конфиденциальности её информации и общим состоянием безопасности.

Сформированная совокупность правовых, организационных и инженерно-технических мероприятий выливается в соответствующую политику безопасности.

Политика безопасности определяет облик системы защиты информации в виде совокупности правовых норм, организационных (правовых) мер, комплекса программно-технических средств и процедурных решений, направленных на противодействие угрозам в целях исключения или минимизации возможных последствий проявления информационных воздействий.

Возможна ситуация, когда для уменьшения риска не существует эффективных и приемлемых по цене мер. В этом случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий.

1.2. ВИДЫ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ЗАЩИТЫ И ИХ ХАРАКТЕРИСТИКА

Угроза – это потенциальные или реальные действия, приводящие к моральному или материальному ущербу.

Угроза безопасности информации – потенциальная возможность нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности.

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Такими действиями являются:

– ознакомление с конфиденциальной информацией различными путями и способами без нарушения её целостности;

– модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;

– разрушение (уничтожение) информации как акт вандализма в целях прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению её конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации. Каждая угроза влечёт за собой определённый ущерб – моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удаётся далеко не всегда.

С учётом этого угрозы могут быть классифицированы по следующим кластерам:

1) по величине принесённого ущерба:

– предельный, после которого фирма может стать банкротом;

– значительный, но не приводящий к банкротству;

– незначительный, который фирма может компенсировать и др.;

2) по вероятности возникновения:
– весьма вероятная угроза;
– вероятная угроза;
– маловероятная угроза;
3) по причинам появления:
– стихийные бедствия;
– преднамеренные действия;
4) по характеру нанесённого ущерба:
– материальный;
– моральный;
5) по характеру воздействия:
– активные;
– пассивные;
6) по отношению к объекту:
– внутренние;
– внешние.

Источниками внешних угроз являются:
– недобросовестные конкуренты;
– преступные группировки и формирования;
– отдельные лица и организации административно-управленческого аппарата.

Источниками внутренних угроз могут быть:
– администрация предприятия;
– персонал;
– технические средства обеспечения производственной и трудовой деятельности.

Соотношение внешних и внутренних угроз на усреднённом уровне можно охарактеризовать так:

82% угроз совершается собственными сотрудниками фирмы либо при их прямом или опосредованном участии;

17% угроз совершается извне – внешние угрозы;

1% угроз совершается случайными лицами.

1.3. МОДЕЛИ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ

Каждый собственник имущества (субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанным имуществом) сталкивается с задачей обеспечения его охраны от различного типа угроз, начиная от банальной кражи до его полного уничтожения. Особую озабоченность при этом у него вызывает построение системы охраны объекта (предприятия), имеющего рассредоточенные на какой-то площади складские и/или производственные помещения, содержащие разнородное защищаемое имущество. Отличительной чертой такого предприятия является протяжён-

ный трудно контролируемый периметр, имеющий, как правило, несколько точек прохода (проезда) персонала (служебного транспорта).

При столкновении с этой проблемой принимается решение организовать защиту имущества построением (модернизацией существующей) системы охраны периметра (СОП) предприятия. Система охраны периметра предприятия по типу используемого оборудования и стоящим задачам относится к системе охранной сигнализации объекта и её построение должно отвечать требованиям нормативных и руководящих документов, приведённых в табл. 1.1.

Вместе с тем в составе СОП кроме технических средств охраны должны применяться инженерные средства, без которых некоторые задачи охраны периметра вообще не реализуемы.

При разработке системы охраны периметра (СОП) предприятия нужно также разработать:

– модель объекта охраны (модель периметра);

– модель угроз (в том числе модель нарушителя) и тактику охраны периметра.

Нарушитель – это лицо, предпринявшее попытку выполнения запрещённых операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, в целях самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Таблица 1.1

Гост	Название
ГОСТ 26342–84	Средства охранной, пожарной и охранно-пожарной сигнализации. Типы, основные параметры и режимы
ГОСТ Р 50775–95	Система тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения
ГОСТ Р 50776–95	Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию
ОСТ 25 1099–83	Средства охранной, пожарной и охранно-пожарной сигнализации. Общие требования и методы испытаний
РД 25.952–90	Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Порядок разработки задания на проектирование
РД 78.145–93 МВД РФ	Средства и комплексы охранной, пожарной и охранно-пожарной сигнализации. Правила производства и приёмки работ
РД 78.146–93 МВД РФ	Инструкция. О техническом надзоре за выполнением проектных и монтажных работ по оборудованию объектов средствами охранной сигнализации
РД 78.147–93 МВД РФ	Единые требования по технической укреплённости и оборудованию сигнализацией охраняемых объектов

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

При разработке модели нарушителя определяются:

- предположения о категориях лиц, к которым может принадлежать нарушитель;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащённости (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей.

Нарушители могут быть *внутренними* (из числа персонала) или *внешними* (посторонними лицами).

Можно выделить несколько основных мотивов нарушений:

- безответственность;
- самоутверждение;
- вандализм;
- принуждение;
- месть;
- корыстный интерес;
- идейные соображения.

При нарушениях, вызванных безответственностью, пользователь производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве случаев это следствие некомпетентности или небрежности.

Основная цель нарушителя в рассматриваемом варианте заключается в скрытном преодолении зоны периметра предприятия для получения несанкционированного доступа (НСД) к охраняемому имуществу собственника. Способ и время, затраченное им на преодоление зоны периметра, прямо зависят от его осведомлённости о возможностях СОП предприятия, технической и физической подготовленности, а также от конечных целей вторжения.

Для определения требуемого уровня защищённости периметра предприятия (его способности противостоять действиям нарушителя) необходимо формирование базовой модели нарушителя, на способности и возможности которого должна ориентироваться создаваемая СОП.

Под моделью нарушителя понимается его описательная характеристика, отражающая его возможный моральный облик, уровень физической подготовленности, знаний, обученности и оснащённости, которые дают возможность оценить степень его способности и заинтересованности в преодолении зоны периметра предприятия, с одной стороны, а с другой – определить допустимый уровень инженерно-технической подготовленности рубежей охраны зоны периметра.

Таблица 1.2

Категория	Тип нарушителя	Характеристика	Физподготовка	Знания о возможностях ТСО	Оснащённость	Примечание
1	Профессионал	Очень опасен. Способен добывать сведения об инженерно-технических средствах охраны инженерно-технических средствах охраны (ИТСО), планировать и готовить вторжение. Действует в одиночку, как правило, не интересуется материальными ресурсами. Опасается огласки	Отличная	Высокие	Специальный набор средств, предназначенный для НСД, недоступен к свободному приобретению	Тренируется государством и используется в его интересах. Защита от его проникновения – безнадёжное дело, это по силам государственным структурам
2	Наёмник (любитель)	Опасен. Способен на нелогичные действия, имеет зачатки плановости действий, может собирать сведения об ИТСО. Действует как в одиночку, так и группой. Интересует весь спектр целей вторжения	Достаточная	Хорошие	Подобранный под задачу НСД набор доступных, но усовершенствованных или самодельных средств	Его услуги стоят дорого – цель его НСД на предприятие должна оправдывать затраты на его наём

3	Безработный (дилетант)	Умеренно опасен. Вторжение планируется на дилетанском уровне по сценарию героев популярных фильмов. Действует, как правило, в одиночку. Интересуют либо материальные, либо информационные ресурсы	Удовлетворительная	Слабые	Бытовые средства, легко доступные для приобретения в магазине	Остро нуждающийся в средствах – услуги его дёшевы. Может преследовать свои цели по обогащению
4	Бытовой (хулиган, наркоман, алкоголик)	Слабо опасен. Действует импульсивно, на основании обрывочных данных о возможной наживе. Действует как в одиночку, так и группой. Интересуют главным образом материальные (финансовые) ценности. Рассчитывает на силовые приёмы	Плохая	Отсутствуют	Подручные средства (что под руку попалось)	Совершает НСД из хулиганских целей либо в целях обогащения. Услуги его очень дёшевы
5	Сотрудник предприятия	Опасен. Способен добывать сведения об ИТСО, планировать и готовить НСД, произвести саботаж ТСО. Действует скрытно, в рабочее время, как в одиночку, так и группой. Интересуют либо материальные, либо информационные ресурсы, но малых размеров, позволяющих их пронос (провоз) через КПП. Может привлекать внешних пособников	Плохая	Высокие	Подобранный под задачу НСД набор доступных, но усовершенствованных или самодельных средств	Остро нуждающийся в средствах. Его услуги стоят дорого – цель его НСД на предприятие должна оправдывать затраты на его наём и потерю работы. Либо преследует свои цели по обогащению

В таблице 1.2 приведены типовые модели нарушителя для различных категорий лиц. На основании статистики нарушений режима, установленного на предприятии, и анализа окружающей его криминогенной обстановки, а также оценки возможностей круга заинтересованных в НСД к охраняемому имуществу лиц (организаций), составляется модель наиболее вероятного нарушителя.

Такая модель наделяется максимальными для выбранного типа способностями и возможностями по преодолению зоны периметра. Созданная модель нарушителя принимается как базовая и относительно неё проходит разработка модели угроз.

Модель угроз представляет собой перечень возможных действий (целей и способов их достижения) нарушителя по преодолению зоны периметра предприятия (распределённого объекта охраны).

Под целью вторжения понимается конечная цель нарушителя, реализуемая им после преодоления зоны периметра. Их возможный спектр достаточно широк – от простой кражи до террористических действий, он прямо зависит от типа охраняемого имущества.

Определение целей вторжения на территорию предприятия, облика возможного нарушителя и наиболее вероятных сценариев его действий даёт возможность сформировать требования к инженерно-техническим средствам системы охраны периметра, при реализации которых возможно её эффективное противостояние.

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определённые ресурсы.

При формировании модели угроз в рассматриваемом случае необходимо учитывать только те угрозы охраняемому имуществу предприятия, которые включают несанкционированное преодоление зоны его периметра нарушителем, обладающим возможностями сформировавшей его базовой модели. Здесь полезными могут быть натурные испытания по количественной оценке возможностей нарушителя, например, времени преодоления внешнего ограждения заданной конструкции или зоны отчуждения, оборудованной инженерными средствами задержания, и т.п. При этом, как правило, исходят из принципа «хуже быть не может», т.е. если созданная СОП в состоянии противостоять (обнаружить) нарушителю базовой модели, то она сможет противостоять всем типам нарушителей, обладающих меньшим уровнем подготовленности по какому-нибудь параметру.

2. ОСНОВНЫЕ НАПРАВЛЕНИЯ, ПРИНЦИПЫ И УСЛОВИЯ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В основе деятельности по организации защиты информации на предприятии лежит совокупность основных принципов, включающая в себя:

– принцип комплексного подхода – эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

– принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);

– принцип персональной ответственности – наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

– непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению её эффективности;

– неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

2.2. ОСНОВНЫЕ ПОДХОДЫ И ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Успешное решение комплекса задач по защите информации не может быть достигнуто без создания единой основы, так называемого «активного кулака» предприятия, способного концентрировать все усилия и имеющиеся ресурсы для исключения утечки конфиденциальной информации и недопущения возможности нанесения ущерба предприятию. Таким «кулаком» призвана стать система защиты информации на предприятии, создаваемая на соответствующей нормативно-методической основе и отражающая все направления и специфику деятельности данного предприятия.

Под системой защиты информации понимают совокупность органов защиты информации (структурных подразделений или должностных лиц предприятия), используемых ими средств и методов защиты информации, а также мероприятий, планируемых и проводимых в этих целях.

Для решения организационных задач по созданию и обеспечению функционирования системы защиты информации используются несколько основных подходов, которые вырабатываются на основе существующей нормативно-правовой базы и с учётом методических разработок по тем или иным направлениям защиты конфиденциальной информации.

Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищённости информационных ресурсов предприятия с учётом устремлённости конкурирующих организаций к овладению конфиденциальной информацией и тем самым нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учётом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищённости информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также на деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

При создании системы защиты информации, в первую очередь, учитываются наиболее важные, приоритетные направления деятельности предприятия, требующие особого внимания. Предпочтение также отдаётся новым, перспективным направлениям деятельности предприятия, которые связаны с научными исследованиями, новейшими технологиями, формирующими интеллектуальную собственность, а также развивающимся международным связям. В соответствии с названными приоритетами формируется перечень возможных угроз информации, подлежащей защите, и определяются конкретные силы, средства, способы и методы её защиты.

К организации системы защиты информации с позиции системного подхода выдвигается ряд требований, определяющих её целостность, стройность и эффективность.

Система защиты информации должна быть:

– централизованной – обеспечивающей эффективное управление системой со стороны руководителя и должностных лиц, отвечающих за различные направления деятельности предприятия;

– плановой – объединяющей усилия различных должностных лиц и структурных подразделений для выполнения стоящих перед предприятием задач в области защиты информации;

– конкретной и целенаправленной – рассчитанной на защиту абсолютно конкретных информационных ресурсов, представляющих интерес для конкурирующих организаций;

– активной – обеспечивающей защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;

– надёжной и универсальной – охватывающей всю деятельность предприятия, связанную с созданием и обменом информацией.

2.3. ОСНОВНЫЕ МЕТОДЫ, СИЛЫ И СРЕДСТВА, ИСПОЛЬЗУЕМЫЕ ДЛЯ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

Один из важнейших факторов, влияющих на эффективность системы защиты конфиденциальной информации, – совокупность сил и средств предприятия, используемых для организации защиты информации.

Силы и средства различных предприятий отличаются по структуре, характеру и порядку использования. Предприятия, работающие с конфиденциальной информацией и решающие задачи по её защите в рамках повседневной деятельности на постоянной основе, вынуждены с этой целью создавать самостоятельные структурные подразделения и использовать высокоэффективные средства защиты информации. Если предприятия лишь эпизодически работают с конфиденциальной информацией в силу её небольших объёмов, вместо создания подразделений они могут включать в свои штаты отдельные должности специалистов по защите информации. Данные подразделения и должности являются органами защиты информации.

Предприятия, работающие с незначительными объёмами конфиденциальной информации, могут на договорной основе использовать потенциал более крупных предприятий, имеющих необходимое количество квалифицированных сотрудников, высокоэффективные средства защиты информации, а также большой опыт практической работы в данной области.

Ведущую роль в организации защиты информации на предприятии играет руководитель предприятия, а также его заместитель, непосредственно возглавляющий эту работу.

Руководитель предприятия несёт персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесённых к конфиденциальной информации, и утрат носителей информации. Он обязан:

– знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;

– определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;

– проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;

– оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

Заместитель руководителя предприятия обязан постоянно изучать все стороны и направления деятельности предприятия для принятия своевременных мер по защите информации; руководить работой службы безопасности (иных структурных подразделений, решающих задачи по защите информации); выполнять другие функции по организации защиты информации в ходе проведения предприятием всех видов работ. На предприятиях для организации работ по защите информации могут создаваться следующие основные виды структурных подразделений:

– режимно-секретные;

– подразделения по технической защите информации и противодействию иностранным техническим разведкам;

– подразделения криптографической защиты информации;

– мобилизационные;

– подразделения охраны и пропускного режима.

Функции, возлагаемые на перечисленные подразделения, определяются решением (приказом) руководителя предприятия и отражаются в соответствующих положениях.

По решению руководителя предприятия данные подразделения организационно могут объединяться в службу безопасности, руководитель которой в некоторых случаях может быть наделён статусом заместителя руководителя предприятия и полномочиями должностного лица, осуществляющего руководство работой структурных подразделений предприятия, деятельность которых связана с использованием и защитой информации.

Режимно-секретное подразделение, мобилизационное подразделение и подразделение по технической защите информации и противодействию иностранным техническим разведкам создаются на предприятиях, выполняющих работы с использованием сведений, составляющих государственную тайну (вне зависимости от наличия на предприятии иной информации с ограниченным доступом).

Режимно-секретное подразделение является основным структурным подразделением предприятия и решает задачи организации, координации и контроля деятельности других структурных подразделений (персонала предприятия) по обеспечению защиты сведений, составляющих государственную тайну. На предприятиях, не выполняющих работы со сведениями, составляющими государственную тайну, для решения аналогичных задач в отношении других видов информации с ограниченным доступом создаётся и функционирует служба безопасности (служба защиты информации).

Подразделение по технической защите информации и противодействию иностранным техническим разведкам решает задачи организации и проведения комплекса технических мероприятий, направленных на исключение или существенное затруднение добывания иностранными разведками с помощью технических средств сведений, отнесённых к конфиденциальной информации и подлежащих защите.

Подразделение криптографической защиты информации создаётся в целях предотвращения утечки конфиденциальной информации при её передаче по открытым каналам (линиям) связи с помощью технических средств, а также при использовании локальных вычислительных сетей, имеющих выход за пределы территории предприятия.

Подразделение охраны и пропускного режима создаётся в целях предотвращения несанкционированного (бесконтрольного) пребывания на территории и объектах предприятия посторонних лиц и транспорта, нанесения ущерба предприятию путём краж (хищений) с территории предприятия материальных средств и иного имущества. В некоторых случаях для решения задач охраны и пропускного режима на предприятиях могут создаваться отдельные самостоятельные подразделения.

Мобилизационное подразделение решает задачи всесторонней подготовки предприятия к работе в условиях военного времени, призыва и поступления мобилизационных людских и материальных ресурсов.

Кроме перечисленных подразделений предприятия к работе по организации защиты информации могут привлекаться и иные структурные подразделения, для которых выполнение мероприятий по защите информации не является основной функцией.

К таким подразделениям относятся кадровый орган, орган юридической службы (юрисконсульт), орган психологической и воспитательной работы, пресс-служба предприятия и др. Особо необходимо отметить важность участия в организации защиты информации производственных, так называемых «тематических» структурных подразделений (отдельных должностных лиц), которые создают продукцию и товары или оказывают услуги (например, производство стрейч-плёнки), и в связи с этим самым непосредственным образом взаимодействуют с другими предприятиями и органами государственной власти.

Для проведения работ по организации защиты информации используются также возможности различных нештатных подразделений предприятия, в том числе коллегиальных органов (комиссий), создаваемых для решения специфических задач в этой области. В их числе – постоянно действующая техническая комиссия, экспертная комиссия, комиссия по рассекречиванию носителей конфиденциальной информации, комиссия по категорированию объектов информатизации и др.

Чтобы добиться максимальной эффективности при решении задач защиты информации, наряду с возможностями упомянутых штатных и нештатных подразделений (должностных лиц) необходимо использовать имеющиеся на предприятии средства защиты информации.

Под средствами защиты информации понимают технические, криптографические, программные и другие средства и системы, разработанные и предназначенные для защиты конфиденциальной информации, а также средства, устройства и системы контроля эффективности защиты информации.

Технические средства защиты информации – устройства (приборы), предназначенные для обеспечения защиты информации, исключения её утечки, создания помех (препятствий) техническим средствам доступа к информации, подлежащей защите.

Криптографические средства защиты информации – средства (устройства), обеспечивающие защиту конфиденциальной информации путём её криптографического преобразования (шифрования).

Программные средства защиты информации – системы защиты средств автоматизации (персональных электронно-вычислительных машин и их комплексов) от внешнего (постороннего) воздействия или вторжения.

Эффективное решение задач организации защиты информации невозможно без применения комплекса имеющихся в распоряжении руководителя предприятия соответствующих сил и средств. Вместе с тем определяющую роль в вопросах организации защиты информации, применения в этих целях сил и средств предприятия играют методы защиты информации, определяющие порядок, алгоритм и особенности использования данных сил и средств в конкретной ситуации.

Методы защиты информации – это применяемые в целях исключения утечки информации универсальные и специфические способы использования имеющихся сил и средств (приёмы, меры, мероприятия), учитывающие специфику деятельности по защите информации.

Общие методы защиты информации подразделяются на правовые, организационные, технические и экономические.

Методы защиты информации с точки зрения их теоретической основы и практического использования взаимосвязаны. Правовые методы регламентируют и всесторонне нормативно регулируют деятельность по защите информации, выделяя, прежде всего, её организационные направления. Тесную связь организационных и правовых методов защиты информации можно показать на примере решения задач по исключению утечки конфиденциальной информации, в частности относящейся к коммерческой тайне предприятия, при его взаимодействии с различными государственными и территориальными инспекторскими и надзорными органами. Эти органы в соответствии с предоставленными им законом полномочия-

ми осуществляют деятельность по получению (истребованию), обработке и хранению информации о предприятиях и гражданах (являющихся их сотрудниками).

Передача информации, в установленном порядке отнесённой к коммерческой тайне или содержащей персональные данные работника предприятия, должна осуществляться на основе договора, предусматривающего взаимные обязательства сторон по нераспространению (неразглашению) этой информации, а также необходимые меры по её защите.

Организационные механизмы защиты информации определяют порядок и условия комплексного использования имеющихся сил и средств, эффективность которых зависит от применяемых методов технического и экономического характера.

Технические методы защиты информации, используемые в комплексе с организационными методами, играют большую роль в обеспечении защиты информации при её хранении, накоплении и обработке с использованием средств автоматизации. Технические методы необходимы для эффективного применения имеющихся в распоряжении предприятия средств защиты информации, основанных на новых информационных технологиях.

Среди перечисленных методов защиты информации особо выделяются организационные методы, направленные на решение следующих задач:

– реализация на предприятии эффективного механизма управления, обеспечивающего защиту конфиденциальной информации и недопущение её утечки;

– осуществление принципа персональной ответственности руководителей подразделений и персонала предприятия за защиту конфиденциальной информации;

– определение перечней сведений, относимых на предприятии к различным категориям (видам) конфиденциальной информации;

– ограничение круга лиц, имеющих право доступа к различным видам информации в зависимости от степени её конфиденциальности;

– подбор и изучение лиц, назначаемых на должности, связанные с конфиденциальной информацией, обучение и воспитание персонала предприятия, допущенного к конфиденциальной информации;

– организация и ведение конфиденциального делопроизводства;

– осуществление систематического контроля за соблюдением установленных требований по защите информации.

Приведённый перечень организационных методов не является исчерпывающим и, в зависимости от специфики деятельности предприятия, степени конфиденциальности используемой информации, объёма выполняемых работ, а также опыта работы в области защиты информации, может быть дополнен иными методами.

3. ОРГАНИЗАЦИЯ СЛУЖБЫ БЕЗОПАСНОСТИ

3.1. ФУНКЦИИ, ЗАДАЧИ И ОСОБЕННОСТИ СЛУЖБЫ БЕЗОПАСНОСТИ ОБЪЕКТА

Многогранность сферы обеспечения безопасности и защиты информации требует создания специальной службы, осуществляющей реализацию специальных защитных мероприятий.

Структура, численность и состав службы безопасности предприятия (фирмы, компании и т.д.) определяются реальными потребностями предприятия и степенью конфиденциальности её информации. В зависимости от масштабов и мощности организации деятельность по обеспечению безопасности предприятия и защиты информации может быть реализована от абонентного обслуживания силами специальных центров безопасности до полномасштабной службы компании с развитой штатной численностью.

Основными задачами службы безопасности предприятия являются обеспечение безопасности предприятия, производства, продукции и защита коммерческой, промышленной, финансовой, деловой и другой информации, независимо от её назначения и форм при всём многообразии возможных каналов её утечки и различных злонамеренных действий со стороны конкурентов.

Основные задачи службы безопасности:

– обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;

– 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, заседания, связанные с деловым сотрудничеством как на национальном, так и на международном уровнях;

– 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.

Общие функции службы безопасности:

– организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, смежниками, партнёрами и посетителями;

– руководит работами по правовому и организационному регулированию отношений по защите коммерческой тайны;

– участвует в разработке основополагающих документов в целях закрепления в них требований обеспечения безопасности и защиты коммерческой тайны, в частности Устава, Коллективного договора, Правил внутреннего трудового распорядка, Положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

– разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся коммерческой тайной, при всех видах работ, организует и контролирует выполнение требований «Инструкции по защите коммерческой тайны»;

– изучает все стороны коммерческой, производственной, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки конфиденциальной информации, ведёт учёт и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций о деятельности предприятия и его клиентов, партнёров, смежников;

– организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности предприятия;

– разрабатывает, ведёт, обновляет и пополняет «Перечень сведений, составляющих коммерческую тайну» и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

– обеспечивает строгое выполнение требований нормативных документов по защите коммерческой тайны;

– осуществляет руководство службами и подразделениями безопасности подведомственных предприятий, организаций, учреждений и других в части оговорённых в договорах условиях по защите коммерческой тайны;

– организует и регулярно проводит учёбу сотрудников предприятия и службы безопасности по всем направлениям защиты коммерческой тайны, добиваясь, чтобы к защите коммерческих секретов был глубоко осознанный подход;

– ведёт учёт сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение конфиденциальных документов;

– ведёт учёт выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

– поддерживает контакты с правоохранительными органами и службами безопасности соседних предприятий в интересах изучения криминогенной обстановки в районе (зоне).

3.2. ПРИНЦИПЫ ОРГАНИЗАЦИИ СЛУЖБЫ БЕЗОПАСНОСТИ ОБЪЕКТА. ТИПОВАЯ СТРУКТУРА СЛУЖБЫ БЕЗОПАСНОСТИ

Для защиты коммерческих секретов предприятия создают собственные службы безопасности, важной предпосылкой создания которых является разработка их структуры, состава, положений о подразделениях и должностных инструкций для руководящего состава и сотрудников.

Служба безопасности (СБ) является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю предприятия. Такая структура управления системой безопасности, имеющая чёткую вертикаль, характерна для области обеспечения безопасности, где требуется определённость, чёткие границы, регламентация отношений на всех уровнях – от рядового сотрудника до менеджеров высшего звена. Как показывает практика, только на предприятиях, где проблемы безопасности находятся под постоянным контролем руководителя предприятия, достигаются наиболее высокие результаты.

Возглавляет службу безопасности начальник службы в должности заместителя руководителя предприятия по безопасности. При этом руководитель СБ должен обладать максимально возможным кругом полномочий, позволяющим ему влиять на другие подразделения и различные области деятельности предприятия, если этого требуют интересы безопасности.

3.3. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ СЛУЖБЫ БЕЗОПАСНОСТИ

Сотрудники подразделений службы безопасности в целях обеспечения защиты сведений, составляющих коммерческую тайну, имеют право:

– требовать от всех сотрудников предприятия, партнёров, клиентов строгого и неукоснительного выполнения требований нормативных документов или договорных обязательств по защите коммерческой тайны;

– вносить предложения по совершенствованию правовых, организационных и инженерно-технических мероприятий по защите коммерческой тайны.

Сотрудники службы безопасности обязаны:

– осуществлять контроль за соблюдением «Инструкции по защите коммерческой тайны»;

– докладывать руководству о фактах нарушения требований нормативных документов по защите коммерческой тайны и других действий, которые могут привести к утечке конфиденциальной информации или утрате документов или изделий;

– не допускать неправомерного ознакомления с документами и материалами с грифом «Коммерческая тайна» посторонних лиц.

Сотрудники службы безопасности несут ответственность за личное нарушение безопасности коммерческой тайны и за неиспользование своих прав при выполнении функциональных обязанностей по защите конфиденциальных сведений сотрудниками предприятия.

Структура службы безопасности и её численность зависят от формы собственности предприятия, вида его производственной деятельности, места предприятия на рынке товаров и услуг, числа сотрудников, наличия на предприятии крупных материальных ценностей, взрыво- и пожароопасных веществ, информации, составляющей государственную тайну, активности конкурентов и криминальных структур. Поэтому можно выделить основные структурные подразделения, которые должны присутствовать в большинстве случаев при организации СБ на крупных промышленных государственных, акционерных предприятиях, в промышленно-финансовых группах, холдингах и т.п.

Типовая структура СБ приведена в табл. 3.1.

3.1. Типовая структура СБ

Подразделение СБ	Внутренняя структура	Функции
Отдел физической охраны и режима	Группа охраны Группа сопровождения Тревожная группа Группа инженерно-технической защиты Группа режима Бюро пропусков	Обеспечение физической безопасности людей и материальных ценностей Обеспечение пропускного и внутриобъектового режима
Отдел безопасности внешней деятельности	Разведывательная группа Контрразведывательная группа Аналитическая группа	Сбор и анализ разведывательной информации
Отдел защиты информации	Группа технической защиты информации Группа конфиденциального делопроизводства	Предотвращение утечки конфиденциальной информации с охраняемого объекта
Отдел психологической безопасности	–	Проверка благонадёжности сотрудников, защита от «внутреннего» нарушителя

Приведённая структура службы безопасности не универсальна и должна корректироваться под определённую организацию.

Состав и функции, задачи, права и обязанности подразделений службы безопасности определяются соответствующими Положениями и Должностными инструкциями, которые регламентируют в целом деятельность службы безопасности объекта.

3.4. СПОСОБЫ И ФОРМЫ ВЗАИМОДЕЙСТВИЯ СЛУЖБЫ БЕЗОПАСНОСТИ ОБЪЕКТА С ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

Особое внимание в процессе повседневной деятельности следует уделять постоянному взаимодействию службы безопасности с правоохранительными органами.

Взаимодействие между службой безопасности и правоохранительными органами осуществляется в целях:

- защиты от преступных посягательств на имущество и инфраструктуру объекта средствами и методами оперативно-розыскной, уголовно-процессуальной и частной сыскной деятельности;
- защиты организации и его сотрудников от преступных посягательств средствами и методами охранной деятельности;
- разработки и внедрения средств инженерно-технической защиты организации и его инфраструктуры;
- обучения и повышения квалификации сотрудников служб безопасности организации.

В процессе предупреждения и раскрытия преступлений средствами и методами оперативно-розыскной, уголовно-процессуальной и частной сыскной деятельности определяются следующие направления взаимодействия:

1) обмен информацией:

- о подготавливаемых и совершённых преступных посягательствах на безопасность предприятия, о причастных к ним лицах;
- о лицах – участниках организованных преступных структур, пытающихся вступить в договорные (в том числе трудовые) отношения с предприятием;
- о фактах совершённых и нераскрытых преступлений;
- об организованных преступных структурах, деятельность которых причинила (может повлечь) ущерб безопасности предприятия;
- о лицах, объявленных в розыск в связи с совершением преступления;
- о применяемых преступниками способах совершения преступлений и приёмах их маскировки, о других действиях, препятствующих осуществлению задач уголовного судопроизводства;

- о признаках и реквизитах поддельных документов и денежных знаков, использующихся для совершения преступлений;
- о появлении иных обстоятельств, содержащих возможную угрозу безопасности организации;
- о материалах научных исследований и методических разработок;
- о предложениях по повышению эффективности информационного обеспечения правовых, организационных и методических мер борьбы с преступной деятельностью;

2) совместное участие в предупреждении и пресечении готовящихся преступных посягательств, реализуемое путём:

- разработки и реализации планов совместных мер в случае угрозы насильственных преступных посягательств на предприятие и его персонал; совместного участия в планировании и организации профилактической работы по борьбе с преступлениями и другими правонарушениями (на договорной основе);
- оказания службой безопасности правоохранительным органам содействия в выявлении и пресечении действий лиц, совершающих преступления ненасильственного характера;
- создания службой безопасности условий для выявления информации, имеющей доказательственное значение, и её фиксации в установленном законом порядке;

3) оказание службой безопасности содействия правоохранительным и следственным органам в процессе расследования преступлений, посягающих на интересы предприятия, путём:

- подготовки службой безопасности материалов, служащих поводом для возбуждения уголовного дела;
- участия службы безопасности в расследовании по возбуждённым уголовным делам на основании п. 7 ст. 3 Закона о частной детективной и охранной деятельности;
- направления службой безопасности правоохранительным органам информации, которая может иметь отношение к расследованию по возбуждённым уголовным делам;
- оказания службой безопасности помощи организационного и технического характера в процессе осуществления на предприятии следственных действий.

Направления взаимодействия в процессе защиты предприятия и его сотрудников от преступных посягательств средствами и методами охранной деятельности (реализуются подразделениями вневедомственной охраны МВД России на договорной основе):

- охрана имущества предприятия сотрудниками органов внутренних дел;
- оказание содействия предприятию в разработке мер по обеспечению его имущественной безопасности, а также личной безопасности его работников;

- экспертная оценка состояния средств технической защиты, охранной, тревожной и пожарной сигнализации предприятия, разработка предложений по совершенствованию системы технической защиты;
- оценка уязвимости имущества предприятия от преступных и иных противоправных посягательств, оказание службе безопасности практической и методической помощи по повышению эффективности мер защиты;
- осуществление технического надзора за выполнением проектных и монтажных работ по оборудованию средствами охранной сигнализации, использованием приборов и систем охраны в соответствии с технической документацией, приём их в эксплуатацию, обслуживание и ремонт;
- разработка и внедрение специальных средств инженерно-технической защиты объектов собственности и инфраструктуры предприятия;
- подготовка сотрудников службы безопасности;
- обучение сотрудников службы безопасности тактике задержания правонарушителей, посягающих на охраняемое имущество, порядку осуществления пропускного режима, правилам производства досмотра вещей, транспортных средств, личного досмотра;
- отработка с сотрудниками службы безопасности вводных задач по защите предприятия, организация учебно-тренировочных стрельб;
- участие в комиссиях по приёмке в эксплуатацию охраняемых помещений и здания предприятия;
- участие в выступлениях перед сотрудниками предприятия по вопросам сохранности собственности;
- подготовка помещений и объектов собственности предприятия для последующей передачи их под охрану службы безопасности.

4. ПОДБОР СОТРУДНИКОВ И РАБОТА С КАДРАМИ

При приёме на работу должны быть проверены идентичность личности, заявляемая квалификация, точность и полнота биографических фактов, наличие рекомендаций.

Лиц, которых предполагается принять на работу, связанную с защищаемыми активами или операциями, следует подвергать проверке в части профессиональных навыков и оценки профессиональной пригодности. Рекомендуется выполнять контрольные проверки уже работающих сотрудников регулярно, а также внепланово при выявлении фактов их нештатного поведения, или участия в инцидентах информационной безопасности (ИБ), или подозрений в таком поведении или участии.

Весь персонал организации должен давать письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов. При этом условие о соблюдении конфиденциальности должно распространяться на всю защищаемую информацию, доверенную сотруднику или ставшую ему известной в процессе выполнения им своих служебных обязанностей.

Для внешних организаций требования по ИБ регламентируются положениями, включаемыми в договоры (соглашения).

4.1. ОСНОВНЫЕ КРИТЕРИИ ПРИЁМА НА РАБОТУ, СВЯЗАННУЮ С СОХРАНЕНИЕМ ТАЙНЫ

В целях ограждения кадрового состава от проникновения лиц с противоправными устремлениями на стадии отбора кандидатов на работу осуществляют мероприятия правового, организационного и поискового характера:

а) разработку перечня требований квалификационного и иного характера, предъявляемых при приёме на работу кандидатам на конкретные должности, а также внутреннего нормативного акта, устанавливающего порядок получения и проверки характеризующей кандидата информации;

б) сбор и проверку информации, характеризующей кандидата (в том числе методами частного сыска и тестирования с применением полиграфа);

в) выявление законодательно установленных обстоятельств, препятствующих заключению трудового договора:

- лишение права занимать определённые должности или заниматься определённой деятельностью по приговору суда;
- судимость за совершение преступлений против собственности, хозяйственных и должностных преступлений;

- совершение в течение года административного правонарушения в области торговли и финансов, установленного вступившим в законную силу постановлением органа, уполномоченного рассматривать дела об административных правонарушениях;
- расторжение трудового договора по инициативе администрации в связи с утратой доверия;
- несоответствие действительности представленных кандидатом анкетных данных, сведений о прежних местах работы, занимаемых должностях, об образовании, о квалификации;

г) выявление признаков отрицательной нравственно-психологической и социальной характеристик личности, делающих заключение трудового договора с кандидатом нежелательным (связи с представителями криминального мира; конфликты с законом, правоохранительными органами, кредиторами; характер взаимоотношений с коллегами по прежней работе; злоупотребление алкогольными напитками, употребление наркотиков, токсикомания, увлечение азартными играми).

Следующим этапом выбора подходящего кандидата на работу может быть проведение анкетирования и собеседования. Конечным результатом этих мероприятий является заполненный личный листок по учёту кадров (анкета) и оценочный лист по результатам собеседования.

Анкета может быть не только общей, но и специальной нацеленной на конкретные категории претендентов, а также на освещение тех или иных сторон их биографии. Она обычно содержит вопросы об уровне квалификации, специальных, экономических и управленческих знаниях, организационных навыках, психологических качествах, самостоятельности, общественной активности, сведения о местах работы и причинах увольнений.

Оценочный лист по результатам собеседования содержит общую оценку кандидата, полученную в ходе собеседования на основе оценок по следующим блокам: общеобразовательный уровень, практический опыт, индивидуальные характеристики, а также зафиксированное предложение данному претенденту (возможны следующие: принять на работу, рекомендовать на следующее собеседование, рассмотреть кандидата на другую должность, отказать, зачислить в резерв).

Важным документом, который подписывает сотрудник при приёме на работу, является соглашение с сотрудником о неразглашении конфиденциальной информации предприятия. Продолжением обязанностей сотрудника по неразглашению информации является документ, декларирующий подтверждение сотрудником данных обязательств при увольнении, а именно – заявление о подтверждении обязательств неразглашения конфиденциальной информации предприятия при увольнении.

5. ОРГАНИЗАЦИЯ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

5.1. НАЗНАЧЕНИЕ И ТРЕБОВАНИЯ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

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

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

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

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 фирмы 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 придётся преодолевать злоумышленнику.

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

Внутриобъектовый режим предусматривает следующие основные требования:

– установление чёткого распорядка рабочего времени;

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

– установление порядка приёма 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 приёма помещений под охрану;

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

Работа с представителями сторонних организаций осуществляется в следующем порядке:

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

– в день прибытия приглашённых канцелярия фиксирует их прибытие в журнале учёта посетителей и приглашает специалиста фирмы;

– специалист встречает прибывших, получает в канцелярии ключи от комнаты переговоров и сопровождает туда посетителей. Запрещается приём 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 учёта 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 сдаёт ключи от неё канцелярии.

Перечень предметов, запрещённых к проносу/провозу на территорию организации, перечислен в должностной инструкции начальника смены (начальника караула или наряда) сектора охраны. Этот документ составляется сотрудниками службы безопасности организации за подписью начальника службы безопасности организации. После составления документ визируется сотрудниками юридического отдела организации.

5.2. ОПРЕДЕЛЕНИЕ ГРАНИЦЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

Контролируемая зона (КЗ) – это территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа. Контролируемая зона может ограничиваться периметром охраняемой территорией частично, охраняемой территорией, охватывающей здания и сооружения, в которых проводятся закрытые мероприятия, частью зданий, комнаты, кабинетом, в которых проводятся закрытые мероприятия. Контролируемая зона может устанавливаться больше чем охраняемая территория, при этом обеспечивающая постоянный контроль за не охраняемой частью территории. В контролируемой зоне посредством проведения технических и режимных мероприятий должны быть созданы условия, предотвращающие возможность утечки из неё конфиденциальной информации.

Постоянная контролируемая зона – это зона, границы которой устанавливаются на длительный срок.

5.1. Требования размеров КЗ по защите перехвата побочных электромагнитных излучений

Тип СО	КЗ, м
1	250
2	100
3	50
4	45
5	40
6	35
7	30
8	20
9	15

Временная зона – это зона, устанавливаемая для проведения закрытых мероприятий разового характера.

Согласно требованиям нормативных документов технической защиты информации (НДТЗИ) должна обеспечиваться контролируемая зона следующих размеров:

– первой категории универсального объекта требуется 50 м контролируемой зоны;

– второй категории объекта требуется 30 м;

– третьей категории объектов требуется 15 м контролируемой зоны.

Также требуется определённый размер контролируемой зоны для разных типов специализированных объектов (СО) (табл. 5.1).

5.3. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, В КОТОРЫХ ЦИРКУЛИРУЕТ ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ

Помещение, в котором циркулирует защищаемая информация, должно находиться в контролируемой зоне. Помещение должно быть оборудовано надёжными автоматическими замками, средствами сигнализации и контроля доступа, постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (ПЭВМ, документов, реквизитов доступа и т.п.).

Уборка помещений с установленными в них ПЭВМ должна производиться с разрешения ответственного, за которым закреплены данные технические средства, или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

В помещениях во время обработки и отображения на ПЭВМ информации ограниченного распространения должен присутствовать только персонал, допущенный к работе с данной информацией. Запрещается приём посетителей в помещениях, когда осуществляется обработка защищаемой информации.

По окончании рабочего дня помещения с установленными защищёнными ПЭВМ, серверами, сетевым и коммутационным оборудованием должны сдаваться под охрану на основании специально разрабатываемой инструкции, утверждаемой руководством службы безопасности организации.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами.

Помещения должны быть обеспечены средствами уничтожения документов.

5.4. АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых ФСТЭК (Гостехкомиссией) России.

Наличие на объекте информатизации действующего «Аттестата соответствия» даёт право обработки информации с уровнем секретности (конфиденциальности) и на тот период времени, который установлен в «Аттестате соответствия».

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счёт побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки информации или воздействия на неё за счёт специальных устройств, встроенных в объекты информатизации.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Аттестация проводится органом по аттестации в установленном порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из следующего основного перечня работ:

– анализ исходных данных по аттестуемому объекту информатизации;

– предварительное ознакомление с аттестуемым объектом информатизации;

– проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения её соответствия требованиям нормативной и методической документации;

– проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

– проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

– проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

– анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

5.5. КАТЕГОРИРОВАНИЕ ПОМЕЩЕНИЙ

Все помещения фирмы в зависимости от назначения и характера совершаемых в них актов, действий или операций разделяются на несколько зон доступности (классов 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 придётся преодолевать злоумышленнику.

Для определения категории помещения создаётся комиссия, состоящая из председателя и не менее трёх членов. В результате действия комиссии создаётся Акт категорирования помещения. Повторные категорирования помещения проводят ежегодно.

5.2. Классификация категорий помещений

Класс категории помещений	Наименование категории	Функциональное назначение	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны	Наличие технических средств охраны
0	Свободная	Зона свободного посещения	Свободный	Свободный	Нет	Нет
1	Наблюдаемая	Зона приёма посетителей	Свободный	Свободный	Ограниченная	Средства наблюдения и записи
2	Регистрационная	Зона служебных помещений и кабинетов сотрудников	Ограниченный служебной необходимостью	Регистрируемый, по разовым пропускам	В отдельных зонах	Средства охраны и контроля
3	Режимная	Зона руководящего состава, специальных подразделений, финансовых служб	Строго ограниченный	Регистрируемый, по разовым пропускам, с сопровождением	Усиленная многозональная	Средства охраны, контроля и наблюдения

Акт категорирования помещения содержит следующие пункты:

– высший гриф секретности информации, циркулирующей в защищаемом помещении;

– объём циркулирующей в помещении информации с высшим грифом секретности;

– основание для категорирования;

– ранее установленная категория;

– установленная категория.

На основании вышеуказанных классов определяются категории помещений в условиях конкретной организации.

5.6. ОБЕСПЕЧЕНИЕ РЕЖИМА В ЗАЩИЩАЕМЫХ ПОМЕЩЕНИЯХ

Обеспечение режима в защищаемом помещении сводится в основном к регламентации доступа и использования технических средств обеспечения производственной и трудовой деятельности и обработки конфиденциальной информации в традиционных или автоматизированных режимах. Она, как правило, проводится силами службы безопасности путём использования простейших организационных мер и доступных для этого технических средств.

Обеспечение режима предусматривает:

– определение категорий помещений;

– определение границ контролируемой зоны;

– определение технических средств, используемых для обработки конфиденциальной информации в пределах контролируемой зоны;

– определение опасных с точки зрения возможности образования каналов утечки информации или способов несанкционированного доступа (НДС) 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 счёт побочных электромагнитных излучений и наводок (ПЭМИН) или специально используемых для этого сигналов;

– организацию системы допуска персонала в контролируемую зону;

– 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.

В рамках системы допуска персонала в контролируемую зону устанавливается следующее:

– право входа в контролируемую зону;

– время входа в контролируемую зону;

– предметы, устройства, средства, механизмы, которые разрешено пронести в контролируемую зону;

– время пребывания в контролируемой зоне;

– предметы, устройства, средства, механизмы, которые разрешено вынести из контролируемой зоны.

В рамках системы допуска к информации устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях; система разграничения доступа, которая предполагает определение для всех пользователей автоматизированной информационной системы информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Допуск сотрудников организации к работе с автоматизированной системой и доступ к её ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком согласно «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам системы», определяемой политикой безопасности организации. Основными пользователями являются сотрудники организации. Уровень полномочий каждого пользователя определяется индивидуально соблюдением следующих требований:

– открытая и конфиденциальная информация размещаются по возможности на различных серверах (это упрощает обеспечение защиты);

– каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями;

– начальник имеет право на просмотр информации своих подчинённых только в установленных пределах в соответствии со своими должностными обязанностями;

– наиболее ответственные технологические операции должны производиться по правилу «в две руки» – правильность введённой информации подтверждается другим должностным лицом, не имеющим права ввода информации.

Все сотрудники, допущенные к работе (пользователи), и обслуживающий персонал должны нести персональную ответственность за нарушения установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Обработка защищаемой информации в подсистемах должна производиться в соответствии с утверждёнными технологическими инструкциями для данных подсистем.

Для пользователей защищённых ПЭВМ (т.е. ПЭВМ, на которых обрабатывается защищаемая информация или располагаются подлежащие защите подсистемы и на которых установлены соответствующие средства защиты) должны быть разработаны необходимые технологические инструкции, включающие требования по обеспечению безопасности информации.

6. РАБОТА С ПОСЕТИТЕЛЯМИ

Отсутствие порядка в работе с посетителями часто становится причиной утечки коммерческой тайны. В числе первоочередных мер – учёт посетителей, порядок посещения ими производственных помещений, порядок ведения переговоров.

Установлением порядка ведения переговоров с посетителями преследуется двоякая цель: во-первых, не допустить утечки коммерческой тайны, а во-вторых, получить наиболее полную информацию о намерениях посетителей.

Если на предприятии установлен и действует пропускной режим, то учёт посетителей входит в функции бюро пропусков и не составляет особых сложностей. При отсутствии бюро пропусков обязанности по учёту посетителей возлагаются на работников кадровых подразделений или дежурного по комнате приёма посетителей, которые ведут специальный журнал учёта посетителей. Записи в журнале должны делаться лично лицом, ответственным за приём посетителей, так как допуск к ведению журнала посторонних таит в себе угрозу утечки важной информации о связях предприятия.

Обязательным моментом в работе с посетителями является наличие сопровождающих, которые остаются при них весь период нахождения на предприятии. Важным элементом поддержания установленного режима является инструктаж персонала, с требованием не выдавать ни какой информации посетителю без сопровождения.

Минимальный объём правил работы с посетителями, к которым можно отнести:

– все посетители принимаются в строго определённых комнатах;

– при необходимости посещения основных рабочих помещений посетителей не оставляют одних;

– на срок нахождения в помещении посетителя должна быть прекращена работа с документами, не относящимися к данной беседе (документы заранее убираются со стола в сейф), с базами данных ЭВМ, откладываются на время переговоры с сотрудниками и телефонные разговоры по служебным вопросам.

6.1. ПОРЯДОК ВЕДЕНИЯ ПЕРЕГОВОРОВ

После подписания договора о сотрудничестве во время деловых переговоров может возникать необходимость передачи партнёру информации, содержащей коммерческую тайну. Это должно быть оформлено

юридически. Допускаемые в такой ситуации исключения одновременно основываются на следующих обстоятельствах:

– взаимном обмене такой информацией;

– долговременных доверительных отношениях между фирмами и возможности контролировать соблюдение партнёром правил конфиденциальности;

– наличии общего интереса в сохранении производственных секретов и вероятности серьёзных материальных потерь для каждой из участвующих сторон в случае утраты коммерческой информации.

Отдельного внимания требуют заседания с рядом участников, конференции, семинары, где представители фирмы выступают с сообщениями. Наибольшую опасность представляет время «вопросов к докладчику».

Необходимо также обращать внимание на ведение переговоров по телефону, так как кроме подслушивания, существует элементарное выведывание, а приятеля или родственника не нужно отягощать лишней для него информацией.

Телефонные разговоры должны быть кратки. Лучше назначать для переговоров личную встречу и сократить информацию о содержании работы фирмы, которая не входит в рекламный проспект.

Сохранность коммерческой тайны в большей степени зависит от секретаря, лиц, отвечающих за связь с общественностью и прессой, а также за контакты с клиентами. Этих лиц нужно проинструктировать о правилах общения по телефону, в которые, в частности, должны входить:

– исключение сообщения сведений о точном месте нахождения руководителя фирмы, планах его передвижения;

– исключение объяснений, подтверждающих, отрицающих или уточняющих якобы сделанное заявление в прессе, на встрече и т.д.;

– отказ в информации о составе участников переговоров, о заказах, сделках и т.п. на том лишь основании, что звонящий по телефону представляется их участником.

Необходимо ввести правило, чтобы секретарь в отсутствие директора лишь сообщал о готовности передать ему существо поступающей просьбы и координаты обращающегося лица.

7. ОРГАНИЗАЦИЯ ОХРАНЫ ОБЪЕКТА

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

Охрана объекта противостоит сознательным действиям нарушителей.

Целью охраны является обеспечение надёжной защиты зданий, помещений, оборудования, валютных и материальных ценностей, а также личной охраны руководящего состава в обычных и экстремальных условиях.

К задачам охраны относятся:

– предупреждение несанкционированных действий (профилактика) всеми возможными способами;

– своевременное обнаружение несанкционированных действий. Это может быть не только проникновение через периметр объекта, но и любые другие несанкционированные действия, которые может совершить нарушитель, преследуя свои цели;

– задержка проникновения нарушителя. Замедление выполнения им любой поставленной цели. Это время необходимо охране на ответную реакцию;

– пресечение несанкционированных действий. Это – главная задача охраны, т.е. силового вооружённого ответного действия;

– задержание лиц, причастных к подготовке (совершению) диверсии или хищению материальных ценностей с объекта.

Охраняемая зона объекта – участок территории охраняемого объекта, оборудованный физическими барьерами, находящийся под охраной и наблюдением, доступ в который ограничивается и контролируется.

Реализацию жизненно важных интересов любого предприятия (объекта) обеспечивают его корпоративные ресурсы. Эти ресурсы должны быть надёжно защищены от прогнозируемых угроз безопасности.

Для промышленного предприятия такими важными для жизнедеятельности ресурсами, а, следовательно, предметами защиты и охраны являются:

– люди (персонал предприятия);
– важное или дефицитное технологическое оборудование;
– секретная и конфиденциальная документация;
– материальные и финансовые ценности;
– готовая продукция;

– интеллектуальная собственность (ноу-хау);
– средства вычислительной техники (СВТ);
– контрольно-измерительные приборы (КИП) и др.;
– информация конфиденциальная на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях;
– финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, договорные документы и обязательства и т.п.).

Утрата перечисленных ресурсов может привести:
– к большому материальному ущербу;
– созданию угрозы для жизни и здоровья людей;
– разглашению конфиденциальной информации или сведений, содержащих государственную тайну;
– банкротству предприятия.

7.1. СОСТАВ СИСТЕМЫ ОХРАНЫ

Люди и средства инженерной защиты и технической охраны объектов образуют систему охраны.

Подсистема инженерной защиты предназначена для механического воспрепятствования проникновению злоумышленника к объектам защиты. Она включает инженерные конструкции, создающие механические преграды на пути злоумышленника, и комплексы управления доступом людей и автотранспорта на охраняемую территорию.

Подсистема обнаружения должна оповещать сотрудников службы безопасности, прежде всего, охранников, органы вневедомственной охраны, милицию, пожарную охрану о проникновении злоумышленников на охраняемую территорию, о пожаре или иных стихийных бедствиях, защита от которых предусмотрена задачами системы. Основу этой подсистемы составляют технические средства охраны.

Всё шире применяемые телевизионные средства наблюдения составляют основу подсистемы наблюдения. В неё входят также средства дежурного освещения, обеспечивающие необходимый уровень освещённости охраняемой территории в ночное время. Подсистема наблюдения обеспечивает возможность визуального дистанционного контроля за охраняемой территорией и действиями злоумышленников.

Подсистема нейтрализации угроз имеет в своём составе людей и средства для физического и психологического воздействия на злоумышленников, проникших на охраняемую территорию, а также средства тушения пожара.

7.2. ОБЪЕКТЫ ОХРАНЫ

Наиболее обширную группу охраняемых объектов составляют стационарные и подвижные (но стационарно установленные) объекты, арендуемые или находящиеся в собственности акционерных предприятий или частных фирм.

Все объекты можно разделить на две большие группы:

1. Особо важные объекты – предприятия, через которые проходят материальные ценности (МЦ) стратегического значения (ядерные и оружейные материалы; токсичные, наркотические и отравляющие вещества; энергоносители; оружие и боеприпасы и т.д.) особо высокой денежной (дензнаки, драгметаллы и т.д.), информационной, культурно-исторической или духовно-нравственной ценности, когда возможный ущерб максимален, а по значению и масштабам нарушение режима движения МЦ может иметь катастрофические последствия трансграничного, федерального или регионального уровней.

2. Промышленно-коммерческие объекты – предприятия, компании, банки, корпорации и т.д., характеризующиеся тем, что возможный ущерб от нарушения движения МЦ носит имущественный, в основном, коммерческий характер, приводящий к финансово-экономическим потерям и снижению эффективности жизнедеятельности хозяйствующих субъектов (владельцев) предприятия.

Также охраняемые стационарные объекты можно классифицировать следующим образом:

1. По размеру объекта, площади его территории:

а) малые объекты (до 100 $м^2$) – квартиры, малые офисы, отдельно стоящие торговые палатки и ларьки, торговые точки, расположенные в пристройках зданий (например, в одной из проходных арок административного или жилого здания), в бывших служебных помещениях и т.д.;

б) средние объекты (от 100 до 500 $м^2$) – крупногабаритные квартиры в домах улучшенной планировки, частные дома с надворными постройками и приусадебным участком, отдельно стоящие или примыкающие к другим зданиям офисы вместе со складами и производственными помещениями, крупные пункты обмена валюты, небольшие коммерческие банки, автостоянки вместимостью до 50…60 автомашин и т.д.;

в) большие стационарные объекты (500…4000 $м^2$) – средние предприятия с численностью работающих до 300…400 человек, базы хранения продукции, крупные автомобильные стоянки, склады и т.д.;

г) очень большие стационарные объекты (площадью более 4000 $м^2$) – крупные промышленные (акционированные) предприятия, фермерские хозяйства, крупные базы.

2. По режиму работы персонала объекта:

а) объекты, персонал которых работает в одну смену;

б) объекты, работающие в двухсменном режиме;

в) объекты, работающие круглосуточно.

3. По району расположения охраняемого объекта:

а) объекты, расположенные вне основной промышленной, производственной или охраняемой зоны, например, склад предприятия на железнодорожной станции, склад сырья (например, винматериала) на подъездных путях предприятия;

б) объекты в отдельно стоящих зданиях или занимающие часть другого помещения или территории, например, несколько комнат или квартир в доме, этаж или крыло здания, часть территории ярмарки):

– в производственной зоне;

– на охраняемой или вблизи от охраняемой территории;

– рядом с криминогенными объектами (рынки, рестораны, пивные бары, вокзалы).

4. По технической укреплённости объекта:

а) очень хорошо укреплённые объекты, практически не имеющие уязвимых мест;

б) хорошо укреплённые объекты, имеющие незначительное число уязвимых мест, которые известны охране и контролируются её сотрудниками;

в) слабо укреплённые объекты, имеющие значительное число уязвимых мест, многие из которых охрана не контролирует.

5. По типу охраны:

а) объекты с простым типом охраны (путём периодического обхода охраняемой территории без использования огнестрельного оружия и специальных средств);

б) объекты с усложнённым типом охраны (сотрудники используют специальные средства и служебных собак, часть помещений на охраняемом объекте выведена на пульт централизованного наблюдения);

в) объекты с комбинированным типом охраны (для патрулирования объекта используется автотранспорт, охранники экипированы огнестрельным оружием и специальными средствами, используют собак, наиболее значимые помещения оборудованы средствами видеоконтроля территории объекта).

Эта классификация может быть использована для определения стоимости услуг частной охраны, для прогнозирования криминальных ситуаций на объекте. Для решения этих и других вопросов также следует учитывать вид товарноматериальных ценностей, находящихся на объекте, приспособленность объекта для работы охраны.

7.3. ПОСТЫ ОХРАНЫ И ОБЕСПЕЧЕНИЕ СВЯЗИ

В практике охраны используются два вида постов: стационарный и обходной. На участках со значительной протяжённостью охрана использует вело-, мото- или автопатрули.

Стационарным постом считается такой пост, на котором осуществляется охрана одного обособленного объекта либо нескольких объектов на открытой площадке или ограждённой территории, если общая протяжённость обхода их постовым не превышает 150 м.

В практике охраны следует использовать как открытые, так и закрытые стационарные посты, т.е. такие, на которых охранника не видно со стороны территории, смежной или прилегающей к охраняемому объекту.

Обходным постом считается пост, на котором охрана одного или нескольких объектов осуществляется путём их обхода, когда протяжённость маршрута составляет свыше 150 м, но не более 1500 м.

При выставлении постов надо обеспечить:

а) максимально полный контроль за охраняемым зданием, помещением или территорией (участком местности);

б) возможность визуального контроля охранником одного поста хотя бы части территории соседнего поста;

в) возможность взаимопомощи соседних постов;

г) связь охранников друг с другом и со старшим смены.

В практике охраны применяются следующие приёмы контроля и осмотра охраняемого объекта.

1. Фронтальный осмотр объекта, при котором несколько охранников движутся в одном направлении до границы охраняемого объекта, а затем производят движение в обратную сторону.

2. Осмотр объекта навстречу друг другу, при котором охранники движутся от границы объекта к центру (точке встречи), после чего вновь расходятся в направлении периметра охраняемого объекта.

3. Концентрический и эксцентрический способ контроля и осмотра объекта, при котором один или два охранника движутся по спирали от центра охраняемой территории на периферию, и наоборот.

4. Последовательный осмотр отдельных участков охраняемого объекта по сложной траектории в зависимости от планировки и конструкции объекта.

5. Выборочный осмотр участков объекта в зависимости от значимости хранимых товароматериальных ценностей, наличия на объекте уязвимых мест.

6. Движение по объекту с постоянно меняющимся маршрутом применяется в сложных ситуациях для предупреждения нападения на охранника.

7. Движение по объекту с временными остановками и осмотром уязвимых мест и иных участков с закрытого поста (из засады).

Практически все службы безопасности и охраны в своей деятельности используют радиосвязь для организации взаимодействия и управления сотрудниками.

При охране объектов средства связи должны обеспечивать связь как внутри охраняемого объекта, так и за его пределами. Во избежание нежелательных контактов охранников с криминальными элементами посты на объекте должны быть оборудованы только внутренней связью со старшим смены (или с начальником караула). Если же на охраняемом объекте только один пост, то его следует оборудовать как внутренней связью с участками или отделами предприятия (организации), так и внешней связью. В значительной степени негативных контактов охранников по телефону можно избежать за счёт использования на объекте средств радиосвязи, переговоры, по каналам которой легче контролировать.

В настоящее время для связи чаще всего используется транкинговые системы. Во многих случаях объём и качество услуг на основе данных систем соответствуют требованиям служб безопасности и аренда ресурсов данных систем является единственно возможным решением, особенно где плотность абонентов достаточно высока, а радиочастотный ресурс практически исчерпан.

7.4. ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАНЫ И ВИДЕОНАБЛЮДЕНИЯ ОБЪЕКТА

Для увеличения эффективности охраны на объекте могут использоваться следующие виды технических средств:

- средства задержки;
- средства охранной сигнализации;
- средства контроля доступа;
- устройства тревожной сигнализации;
- приборы, регистрирующие пронос запрещённых материалов и изделий;
- средства наблюдения за помещениями и территорией;
- устройства, контролирующие правильность выполнения своих обязанностей должностными лицами;
- приборы-ловушки;
- средства учёта и накопления данных по вопросам безопасности.

Все перечисленные устройства могут работать независимо и самостоятельно, но могут и объединяться в так называемые интегрированные системы безопасности, а также могут являться составной частью комплексных систем управления зданиями и помещениями.

Система сертификации технических средств защиты и охраны объектов играет большую роль в деле повышения уровня безопасности жизни и деятельности предприятий. Наличие сертификата качества на изделии защитной техники серьёзно повышает его авторитет и конкурентоспособность.

Развитие международной интеграции и кооперации привело к созданию межнациональных стандартов. Так, в последнее время разрабатывается и внедряется в рамках Европейского комитета по стандартизации (CEM) целая серия стандартов на такие изделия, как сейфы, замки повышенной надёжности и секретности, системы контроля доступа, системы охранной сигнализации и т.д.

Подобно тому, как функции, возложенные на физическую охрану, определяют вид и количество постов охраны, так и функции, возлагаемые на технические средства, определят состав этих средств и требования, которые будут заложены в основу проектирования технической системы защиты. Рассмотрим функции, которые могут быть возложены на современные системы технической защиты:

– блокировка помещений и рубежей, которые должны контролироваться с центрального поста охраны;

– обеспечение задержки лиц, не имеющих права беспрепятственного прохода в охраняемые помещения;

– идентификация личности сотрудников и посетителей, которым предоставлено право прохода в охраняемые помещения;

– регистрация попыток проноса на территорию объекта запрещённых веществ и предметов (радиоактивные изотопы, оружие, взрывчатые вещества и пр.);

– контроль целостности коммуникаций и работоспособности аппаратуры системы технической защиты;

– сбор, обработка и отображение в наглядной форме информации, поступающей с охраняемой территории на центральный пункт охраны;

– регистрация попыток нештатного обращения с техническими средствами охраны персонала объекта и посетителей;

– выявление каналов утечки информации с объекта с использованием технических средств;

– контроль правильности несения службы персоналом охраны и регистрация фактов отклонения от предписанного порядка поведения во время охраны;

– накопление оперативной информации по всем событиям, связанным с обеспечением безопасности с иерархией доступа с накопленным сведениям.

Необходимость выполнения вышеперечисленных функций определяет состав требований к техническим средствам охраны и контроля.

8. ОРГАНИЗАЦИЯ ПРОПУСКНОГО РЕЖИМА

8.1. ПОНЯТИЕ ПРОПУСКНОГО РЕЖИМА

Построение надёжной системы безопасности предприятия – сложный и многогранный процесс. Одним из немаловажных факторов обеспечения надёжной защиты объекта является организация и поддержание определённого контрольно-пропускного режима.

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

Контрольно-пропускной режим является одним из ключевых моментов в организации системы безопасности на предприятии. С этих позиций контрольно-пропускной режим представляет собой комплекс организационных мероприятий (административно-ограничительных), инженерно-технических решений и действий службы безопасности.

Организация контрольно-пропускного режима отличается определённой сложностью. Дело в том, что механизм осуществления контрольно-пропускного режима основывается на применении «запретов» и «ограничений» в отношении субъектов, пересекающих границы охраняемых объектов, для обеспечения интересов предприятия. Такой механизм должен быть безупречным с точки зрения соответствия требованиям действующего законодательства.

8.2. ЦЕЛИ И ЗАДАЧИ ПРОПУСКНОГО РЕЖИМА

Контрольно-пропускной режим (как часть системы безопасности) должен соответствовать действующему законодательству, уставу предприятия, а также иным нормативно-правовым актам, регулирующим деятельность предприятия.

Основными целями создания контрольно-пропускного режима являются:

– защита законных интересов предприятия, поддержание порядка внутреннего управления;

– защита собственности предприятия, её рациональное и эффективное использование;

– рост прибылей предприятия;

– внутренняя и внешняя стабильность предприятия;

– защита коммерческих секретов и прав на интеллектуальную собственность.

Контрольно-пропускной режим как часть системы безопасности позволяет решить следующие задачи:

– обеспечение санкционированного прохода сотрудников и посетителей, ввоза (вывоза) продукции и материальных ценностей, ритмичной работы предприятия;

– предотвращение бесконтрольного проникновения посторонних лиц и транспортных средств на охраняемые территории и в отдельные здания (помещения);

– своевременное выявление угроз интересам предприятия, а также потенциально опасных условий, способствующих нанесению предприятию материального и морального ущерба;

– создание надёжных гарантий поддержания организационной стабильности внешних и внутренних связей предприятия, отработка механизма оперативного реагирования на угрозы и негативные тенденции;

– пресечение посягательств на законные интересы предприятия, использование юридических, экономических, организационных, социально-психологических, технических и иных средств для выявления и ослабления источников угроз безопасности предприятия.

Контрольно-пропускной режим можно определить как систему обеспечения нормативных, организационных и материальных гарантий выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину, технологическое лидерство, научные достижения и охраняемую информацию и как совокупность организационно-правовых ограничений и правил, устанавливающих порядок пропуска через контрольно-пропускные пункты сотрудников объекта, посетителей, транспорта и материальных ценностей.

Нормативные гарантии заключаются в толковании и реализации норм права, уяснении пределов их действия, в формировании необходимых правоотношений, определении и обеспечении правомерной деятельности подразделений и работников фирмы для её безопасности, использования ограничительных мер, применения санкций к физическим и юридическим лицам, посягающим на законные интересы фирмы.

Организационные гарантии формируются путём разработки, построения и поддержания высокой работоспособности общей организационной структуры управления процессом выявления и подавления угроз деятельности фирмы, использования эффективного механизма стимулирования её оптимального функционирования, соответствующей подготовки кадров.

Материальные гарантии формируются за счёт выделения и использования финансовых, технических, кадровых, интеллектуальных, информационных и иных ресурсов фирмы, обеспечивающих своевременное выявление, ослабление и подавление источников угрозы, предотвращение и

локализацию возможного ущерба, создание благоприятных условий для деятельности фирмы. Данные гарантии наполняют нормативные и организационные меры безопасности практическим содержанием, создают реальную основу развития культуры безопасности фирмы.

На каждом предприятии должна быть «Инструкция о контрольно-пропускном режиме», определяющая:

– порядок пропуска сотрудников предприятия, командированных лиц, посетителей, клиентов;

– порядок допуска на территорию объекта транспортных средств, вывоза (ввоза) продукции, документов и материальных ценностей;

– виды и группы пропусков, порядок их оформления и выдачи;

– обязанности должностных лиц по поддержанию контрольно-пропускного режима;

– систему учёта и отчётности, порядок хранения пропусков, печатей и шифров и т.п.

8.3. РАЗРАБОТКА ИНСТРУКЦИИ О ПРОПУСКНОМ РЕЖИМЕ

Практическое решение вопросов, связанных с организацией пропускного режима, оформляется в виде «Инструкции о пропускном режиме». Указанная инструкция должна определять систему организационно-правовых охранных мер, устанавливающих разрешительный порядок (режим) прохода (проезда) на объект (с объекта), и может включать:

1. Общие положения. В этом разделе указываются:

– нормативные документы, на основании которых составлялась инструкция;

– определение контрольно-пропускного режима и цель его введения;

– должностные лица, на которых возлагается организация и практическое руководство контрольно-пропускной системой;

– санкции к нарушителям контрольно-пропускного режима;

– требования к оборудованию различных помещений.

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

– перечислить все КПП и их назначение, описание, расположение и установить их единую нумерацию;

– изложить требования к оборудованию КПП;

– установить порядок прохода сотрудников и посетителей на территорию объекта и в категорированные помещения;

– определить права и основные обязанности контролёров КПП;

– установить помещения, где запрещается принимать посетителей и представителей сторонних организаций.

3. Порядок допуска на объект транспортных средств, вывоза продукции, документов и материальных ценностей. В этом разделе указываются:

– порядок допуска на территорию объекта (с объекта) автотранспорта, принадлежащего объекту;

– порядок въезда и стоянки на территории объекта транспорта, принадлежащего сотрудникам на правах личной собственности;

– порядок пропуска автомашин сторонних организаций, прибывших с грузом в адрес объекта в рабочее и нерабочее время;

– порядок вывоза (ввоза) товарно-материальных ценностей;

– правила оформления документов на вывоз (вынос) материальных ценностей с территории объекта.

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

– виды пропусков, их количество и статус;

– описание пропусков;

– порядок оформления и выдачи пропусков;

– порядок замены и перерегистрации пропусков;

– мероприятия при утрате пропуска сотрудником.

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

6. Учёт и отчётность, порядок хранения пропусков, печатей.

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

При разработке инструкции о контрольно-пропускном режиме определяются виды и группы пропусков, которые будут действовать на предприятии.

На крупных предприятиях, как правило, устанавливается несколько видов пропусков. Это могут быть постоянные, временные, разовые и материальные пропуска

8.4. ОФОРМЛЕНИЕ ПРОПУСКОВ

На крупных предприятиях, как правило, устанавливаются следующие виды пропускных документов, дающих право прохода сотрудников и посетителей на территорию фирмы, вноса (выноса), ввоза (вывоза) материальных ценностей:

– удостоверения;

– постоянные, временные, разовые, материальные пропуска.

На удостоверениях и пропусках проставляются печати, предусмотренные правилами режима, и цифровые знаки, определяющие зону доступности, период их действия, право проноса портфелей (кейсов, папок и др.). Период пребывания сотрудников на территории фирмы в рабочее и нерабочее время определяется руководством с проставлением цифрового знака на

удостоверении или пропуске. Образцы удостоверений и пропусков разрабатываются службой безопасности и утверждаются руководством фирмы.

Утверждённые образцы удостоверений личности, пропусков, оттисков цифровых знаков, печатей (штампов), проставляемых на удостоверениях и пропусках, списки с образцами подписей руководителей или уполномоченных лиц, имеющих право подписывать удостоверения и пропуска, передаются начальнику отдела режима и охраны под расписку.

Полная замена удостоверений и постоянных пропусков производится, как правило, через 3 – 5 лет. Каждый год производится перерегистрация с проставлением соответствующей отметки.

Для перерегистрации, замены или изменения пропускных документов ежегодно по состоянию на 1 января в службу безопасности направляются отделом кадров списки сотрудников с указанием должности, фамилии, имени, отчества и наименования документа с соответствующими пометками (круглосуточно, рабочее время с __ по__ , с портфелем, в какую зону и т.п.).

Удостоверения и постоянные пропуска могут выдаваться лицам, не работающим на данной фирме, по отдельному утверждённому руководством списку с указанием учреждения, должности, фамилии, имени, отчества и сопроводительных помет. Эти документы должны постоянно храниться в бюро пропусков (или у уполномоченного лица) и выдаваться посетителю в момент его прибытия. После завершения работы эти лица сдают документы в бюро пропусков.

Образцы бланков пропусков разрабатываются администрацией объекта (службой безопасности). По своему внешнему виду и содержанию пропуска должны отличаться друг от друга и обладать некоторыми степенями защиты. Все виды пропусков, за исключением материальных, оформляются и выдаются бюро пропусков (или иным подразделением) по письменным заявкам. Виды пропусков определяются в зависимости от специфики предприятия.

Постоянные пропуска выдаются сотрудникам объекта, принятым на постоянную работу, а также работникам других организаций, постоянно обслуживающим объект. Постоянные пропуска могут делиться на группы, их количество и назначение определяется инструкцией о контрольно-пропускном режиме. Постоянные пропуска могут храниться как на руках у сотрудников объекта, так и в кабинах на КПП. Постоянные пропуска лиц, убывающих с объекта на длительное время (отпуск, болезнь, командировка и т.п.), сдаются на хранение в бюро пропусков (отдел кадров), а при хранении таких пропусков в кабине КПП на ячейке (где хранится пропуск) делается соответствующая отметка. Пропуска уволенных с работы уничтожаются в установленном порядке.

Временные пропуска выдаются лицам, работающим по контракту, находящимся на временной работе, прикомандированным к предприятию, и хранятся, как правило, на КПП. Срок действия и порядок оформления

временных пропусков определяется инструкцией о контрольно-пропускном режиме. Временные пропуска могут быть с фотографией и без фотографии. Временные пропуска без фотографии действительны только при предъявлении документа, удостоверяющего личность.

Разовые пропуска. Данный пропуск даёт право пройти в сопровождении сотрудника организации в служебные помещения организации. Сопровождение обязан организовать начальник отдела (подразделения), в который прибыл посетитель. Сотрудник, назначенный для сопровождения, прибывает в бюро пропусков и получает пропуск для сопровождения. После завершения работы посетитель сопровождается сотрудником на выход.

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

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

Разовый пропуск действителен для входа на территорию объекта или его подразделения в течение определённого времени.

Контроль за посетившими предприятие по разовому пропуску осуществляется с помощью отметки на оборотной стороне пропуска, где указывается время посещения, заверенное подписью лица, принявшего посетителя.

Разовый пропуск изымается на КПП контролёром при выходе посетителя с объекта и сдаётся в бюро пропусков. О лицах, не вышедших с объекта по истечении срока действия пропуска, контролёр докладывает начальнику (дежурному по КПП) для принятия мер по выяснению причин задержки. Фамилии лиц, посетивших объект по разовому пропуску, могут записываться в специальную книгу учёта.

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

8.5. ОРГАНИЗАЦИЯ ПРОПУСКА НА ОХРАНЯЕМЫЙ ОБЪЕКТ СОТРУДНИКОВ, ПОСЕТИТЕЛЕЙ, ПРЕДСТАВИТЕЛЕЙ КОНТРОЛЬНЫХ И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

Проход сотрудников и посетителей на территорию объекта в категорированные подразделения и обратно осуществляется по установленным на объекте пропускам, через контрольно-пропускные пункты. Пропуск должен являться основным документом, дающим право на проход.

Допуск командированных (посетителей) производится по временным, разовым пропускам в установленные и указанные в пропуске часы, в исключительных случаях – по утверждённым начальником службы безопасности спискам.

Представители средств массовой информации допускаются на объект на общих основаниях в сопровождении представителей администрации.

В нерабочее время, выходные и праздничные дни допуск сотрудников на объект должен быть ограничен и производиться по предварительным заявкам (спискам) руководителей подразделений, завизированным начальником службы безопасности, с предъявлением постоянного пропуска. На предприятиях со сменным режимом работы к пропуску могут выдаваться специальные вкладыши сменности.

Дежурные специальных служб объекта (электрики, сантехники, работники связи и т.д.), работающие посменно, допускаются на территорию объекта в нерабочее время, в выходные и праздничные дни по спискам, подписанным начальниками соответствующих служб и утверждённым начальником службы безопасности.

На основании действующего законодательства и решения администрации отдельные категории лиц пользуются правом прохода на объект без пропуска при предъявлении служебного удостоверения. К ним относятся:

– работники прокуратуры и других правоохранительных служб;

– работники полиции;

– инспектора труда, котлонадзора, энергонадзора по территориальности;

– должностные лица и отдельные категории работников санитарно-эпидемической службы органов здравоохранения, осуществляющие санитарный надзор.

Категории лиц, имеющих право прохода на объект без пропуска (по служебным удостоверениям), должны быть чётко отражены в инструкции о контрольно-пропускном режиме.

В целях осуществления пропускного режима на территории объекта и в его структурных подразделениях приказом руководителя предприятия утверждается перечень категорированных подразделений (помещений), хранилищ. В этих помещениях устанавливаются специальный режим и повышенная ответственность за его соблюдение работниками этих подразделений.

Допуск в эти помещения осуществляется строго по списку, согласованному со службой безопасности. Приём посетителей сторонних организаций и предприятий, как правило, максимально ограничивается.

Во всех помещениях категорированных подразделений должны быть вывешены в застеклённых рамках списки работников, имеющих допуск в эти помещения. Все помещения по окончании работ осматриваются дежурными по подразделениям и лицами, ответственными за их противопожарное состояние. Электроосветительная и электронагревательная аппаратура обесточивается, окна и форточки закрываются, двери запираются на замок и опечатываются. По окончании рабочего дня оборудованные охранной сигнализацией категорированные помещения, спецхрани-

лища, склады и другие объекты закрываются и опечатываются ответственными лицами этих подразделений. Помещения сдаются под охрану. Представитель охраны проверяет сигнализацию в присутствии работников, сдающих помещение. Ключи от этих помещений в опечатанных пеналах сдаются под расписку в специальном журнале.

Получение ключей, вскрытие помещений, оборудованных охранной сигнализацией, производят лица, имеющие допуск на право вскрытия этих помещений с предъявлением постоянного пропуска. Списки лиц, имеющих право вскрывать (закрывать) указанные помещения, с указанием номеров личных печатей, которыми опечатываются помещения, и номеров служебных телефонов подписываются начальником подразделения и утверждаются начальником службы безопасности.

Все лица, пытающиеся пройти через КПП без предъявления пропуска или по чужому, неправильно оформленному пропуску, пронести на объект (с объекта) запрещённые предметы, задерживаются и на объект не допускаются.

8.6. ДОПУСК НА ТЕРРИТОРИЮ ПРЕДПРИЯТИЯ ТРАНСПОРТНЫХ СРЕДСТВ, ВЫВОЗ МАТЕРИАЛЬНЫХ ЦЕННОСТЕЙ

Допуск на территорию (с территории) предприятия транспортных средств, принадлежащих предприятию, производится при предъявлении водителем личного пропуска со специальным шифром или транспортного пропуска и путевого листа. Грузчики и сопровождающие лица, следующие с транспортом, пропускаются через КПП на общих основаниях.

Въезд и стоянка на территории предприятия транспорта, принадлежащего сотрудникам на правах личной собственности, разрешается по специальным спискам.

Автомашины сторонних организаций, прибывшие с грузом в адрес предприятия в рабочее время, допускаются на территорию по служебным запискам. Въезд машин на территорию предприятия производится штатным водителем в сопровождении представителя администрации (грузополучателя).

Железнодорожный транспорт и обслуживающие его бригады пропускаются на предприятие по пропускам установленного образца, по спискам или иным порядком, установленным инструкцией о пропускном режиме. Для пропуска железнодорожного транспорта от подразделения охраны выделяется специальная группа.

Опломбированные вагоны и контейнеры пропускаются через КПП после их внешнего осмотра, если оттиски пломб соответствуют оттискам в сопроводительных документах или накладных. В случаях несоответствия оттисков, обнаружения проломов вагона (контейнера) или обрыва пломбы вагон (контейнер) подлежит вскрытию и осмотру в присутствии представителей администрации и железной дороги.

Вывоз и вынос готовой продукции и других материальных ценностей с территории объекта осуществляется по материальным пропускам установленного образца.

Убедившись в правильности оформления документов и их полном соответствии с вывозимыми ценностями, охранник оставляет на КПП пропуск, ставит на пропуске дату и время вывоза груза, расписывается и даёт разрешение на вывоз материальных ценностей.

Все документы, вывозимые (выносимые) с предприятия материальные ценности регистрируются в бюро пропусков по книге учёта и в течение следующего дня передаются в бухгалтерию. Документы на вывоз (вынос) материальных ценностей должны быть выписаны только на то количество груза (мест, веса и т.п.), которое может быть вывезено (вынесено) одновременно, и действительны только на дату, указанную в разрешительном документе.

Строительные и древесные отходы, макулатуру, металлолом, металлическую стружку рекомендуется вывозить с территории предприятия как материальные ценности. Вывоз с территории объекта различного мусора, земли и снега может производиться без оформления документов, но с обязательной регистрацией на автотранспортном КПП.

8.7. ОБОРУДОВАНИЕ ПРОПУСКНЫХ ПУНКТОВ

Для организации пропускного режима на предприятии оборудуются контрольно-пропускные пункты. Оборудование КПП должно обеспечивать необходимую пропускную способность и возможность тщательной проверки пропусков и документов у проходящих лиц, досмотра всех видов транспорта, провозимых грузов и удовлетворять следующим требованиям:

– исключать возможность несанкционированного проникновения через КПП на объект (с объекта) людей и транспортных средств;

– способствовать сокращению времени на проверку документов, досмотр транспорта и материальных ценностей;

– способствовать исключению (сведению к минимуму) ошибок охранника при пропуске людей и транспорта;

– обеспечивать меры безопасности охранника при досмотре транспортных средств.

Все виды КПП должны быть оборудованы необходимыми видами связи и тревожной сигнализации для вызова резерва охраны. На КПП рекомендуется располагать внутренний телефон и список телефонов администрации предприятия.

КПП для прохода людей. Для контроля за людьми, проходящими на объект и в отдельные здания (помещения), строятся КПП. Каждое КПП рекомендуется оборудовать комнатой для охраны, комнатой для досмотра

граждан, камерой хранения, гардеробом, турникетом с фиксирующими устройствами-запорами.

Размещение помещений определяется проектами и зависит от средств механизации, автоматизации КПП и особенностей предприятия.

В контрольно-пропускном зале устраиваются проходы, которые оборудуются техническими средствами охраны и физическими барьерами. В комплект оборудования, как правило, входят:

- средства механизации, автоматизации системы контроля доступа;
- физические барьеры (ограждения, турникеты, калитки);
- основное и резервное освещение;
- средства связи и тревожной сигнализации;
- системы видеоконтроля.

В качестве средств контроля доступа могут использоваться различные турникеты. Турникеты предназначены для управления потоками людей и регулирования входа (выхода). В последнее время наиболее широкое распространение получили электромеханические турникеты.

Электромеханические турникеты, в отличие от громоздких и неудобных в управлении механических, легко управляются с пульта охранника и могут работать в составе автоматизированной системы контроля доступа.

При выборе турникета нужно иметь в виду, что они бывают «нормально открытые» и «нормально закрытые». «Нормально открытые» турникеты (например, раздвижные, которые до недавнего времени были установлены в российском метро) в мировой практике используются достаточно редко. Они могут ударить проходящего и не позволяют осуществлять эффективный контроль.

Для осуществления надёжного контроля чаще используются «нормально закрытые» турникеты: роторные турникеты-вертушки, турникеты-триподы и калитки.

Калитки применяются для управления потоками людей, организации свободного прохода в одну сторону (на вход или выход) и запрета прохода в другую. Калитки широко используются в магазинах, аэропортах, вокзалах. Применение калиток для контроля доступа неэффективно, это связано с тем, что калитки не разделяют поток людей по одному, так как после открытия калитки через неё могут пройти несколько человек. Калитки могут устанавливаться для организации свободного выхода, в то время как контроль входа доверяют триподам или вертушкам.

Турникеты-триподы с тремя преграждающими планками являются одним из наиболее оптимальных средств для осуществления контроля санкционированного прохода. Триподы имеют современный элегантный вид и легко монтируются. Триподы позволяют осуществлять эффективный контроль доступа, так как разделяют поток людей по одному, обеспечивая при этом высокую пропускную способность. Триподы могут при-

меняться в системах электронных проходных, в том числе в условиях большого потока людей. Для предотвращения возможности подлезть под планки турникета или перепрыгнуть через них на турникете рекомендуется устанавливать специальные датчики, которые срабатывают при попытке несанкционированного прохода.

Роторные турникеты-вертушки применяются в тех случаях, когда необходимо полное перекрытие зоны прохода. Они могут быть различными по высоте – от поясных до турникетов в полный рост, которые конструктивно подобны вращающимся дверям.

Транспортные КПП. В состав транспортного КПП входит досмотровая площадка и служебные помещения. Досмотровая площадка предназначена для размещения автомобилей при их досмотре. Досмотровые площадки могут располагаться как на территории предприятия, так и за её пределами, на территории, непосредственно примыкающей к основным воротам КПП. Досмотровая площадка должна отвечать следующим требованиям:

– иметь достаточную площадь для размещения досматриваемого транспорта, технические средства для обеспечения нормальных условий работы охранника;

– исключать возможность несанкционированного проникновения на объект (с объекта) людей и транспортных средств;

– обеспечивать при установленной интенсивности движения в любое время суток и года досмотр автомобильного транспорта и перевозимых грузов;

– быть изолированной от других сооружений, не имеющих отношения к охране объекта и оборудованию КПП;

– обеспечивать меры безопасности охранника при выполнении своих обязанностей.

Размеры досмотровой площадки устанавливаются в зависимости от габаритов транспорта и перевозимых грузов и могут составлять: 10 – 12 м в длину и 5–6 м в ширину.

На территории, отведённой для строительства досмотровой площадки, производится планировка местности с таким расчётом, чтобы на ней не задерживались дождевые и талые воды. Поперечный уклон досмотровой площадки делается не менее 2% от места выставления охранника в направлении её боковых сторон (перпендикулярно проезжей части). Поверхность досмотровой площадки покрывается бетоном или асфальтом.

На проезжей части площадки выделяется место остановки транспорта для досмотра, ограниченное двумя линиями «СТОП», выполненными белой краской.

Перед въездом на досмотровую площадку с внешней стороны основных и вспомогательных ворот (шлагбаума), не ближе 3 м от них, также наносится поперечная линия и надпись «СТОП». В целях обеспечения безо-

пасности движения транспорта не менее чем в 100 м от ворот с правой стороны или над дорогой устанавливается указательный знак «Движение в один ряд», а в 50 м от ворот – знак ограничения скорости до 5 км/ч.

Транспортные КПП могут оборудоваться светофорами, весами для взвешивания автомобилей, досмотровой ямой или эстакадой для осмотра грузов, механизированными устройствами для автоматического открытия и закрытия ворот с фиксаторами.

Досмотровые площадки по периметру оборудуются физическими барьерами и рубежом сигнализации. Площадки, как правило, выгораживаются просматриваемым забором из металлической сетки или декоративных решёток высотой до 2,5 м. На площадке оборудуются основные и вспомогательные механизированные ворота. Основные ворота устанавливаются на линии основного ограждения объекта, а вспомогательные – на противоположной стороне досмотровой площадки. Вместо ворот могут применяться механизированные шлагбаумы. На автомобильных КПП используются ворота с ограничением и без ограничения габаритов по высоте. По конструкции они могут быть распашными или раздвижными (выдвижными). Распашные ворота должны оборудоваться фиксаторами.

Для регулирования движения транспорта, проходящего через проезды досмотровых площадок КПП, могут применяться двухсекционные светофоры с линзами красного и зелёного цвета.

В состав электромеханического оборудования КПП для автомобильного транспорта обычно включаются:

– электродвигатели, привод ворот;
– концевые выключатели автоматического отключения электродвигателей при полностью закрытых и открытых створках ворот;
– магнитные пускатели электродвигателей;
– электрооборудование светофоров;
– кабельные, силовые линии.

Групповой распределительный щит (щит управления) может устанавливаться в помещении КПП, а при отсутствии здания КПП в специальном металлическом шкафу непосредственно на досмотровой площадке.

9. ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО ОРГАНИЗАЦИОННОЙ ЗАЩИТЕ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

9.1. ОСНОВНЫЕ ЦЕЛИ ПЛАНИРОВАНИЯ

Одно из наиболее важных направлений деятельности предприятия, осуществляющего работу со сведениями конфиденциального характера, – планирование мероприятий по защите конфиденциальной информации. Планирование указанных мероприятий занимает особое место в системе управления деятельностью как предприятия в целом, так и его структурных подразделений (отдельных должностных лиц). Трудно также переоценить значение этого направления в общей системе организационных мер обеспечения информационной безопасности предприятия.

Основными целями планирования мероприятий по защите информации являются:

– организация проведения комплекса мероприятий по защите конфиденциальной информации, направленных на исключение возможных каналов утечки этой информации;

– установление персональной ответственности всех должностных лиц предприятия за решение вопросов защиты информации в ходе производственной и иной деятельности предприятия;

– определение сроков (времени, периода) проведения конкретных мероприятий по защите информации;

– систематизация (объединение) всех проводимых на плановой основе мероприятий по различным направлениям защиты конфиденциальной информации;

– установление системы контроля за обеспечением защиты информации на предприятии, а также системы отчётности о выполнении конкретных мероприятий;

– уточнение (конкретизация) функций и задач, решаемых отдельными должностными лицами и структурными подразделениями предприятия.

Основой для планирования мероприятий по защите информации на предприятии служат:

– требования законодательных и иных нормативных правовых актов по защите конфиденциальной информации, соответствующих нормативно-методических документов федерального органа исполнительной власти (при наличии ведомственной принадлежности), вышестоящей организации, а при планировании мероприятий по защите информации филиалом или представительством предприятия – указания головного предприятия;

– требования заказчиков проводимых предприятием в рамках соответствующих договоров (контрактов) совместных и других работ;

– положения международных договоров (соглашений) и иных документов, определяющих участие предприятия в тех или иных формах международного сотрудничества;

– положения внутренних организационно-распорядительных документов предприятия (приказов, директив, положений, инструкций), определяющих порядок ведения производственной и иной деятельности, а также конкретизирующих вопросы защиты конфиденциальной информации на предприятии;

– результаты комплексного анализа состояния дел в области защиты информации, проводимого службой безопасности (режимно-секретным подразделением) на основании материалов проверок структурных подразделений (филиалов, представительств) предприятия;

– результаты проверок состояния защиты информации, проведённых вышестоящими организации, федеральными органами исполнительной власти (при наличии ведомственной принадлежности) и заказчиками работ (в рамках выполняемых договоров или контрактов), выработанные на основании этих результатов предложения и рекомендации;

– результаты контроля за состоянием защиты информации, проводимого органами безопасности и иными контролирующими органами (в части, их касающейся);

– особенности повседневной деятельности предприятия и специфика выполнения на предприятии работ с использованием различных видов конфиденциальной информации.

Планирование мероприятий по защите конфиденциальной информации проводится одновременно с планированием основной производственной и иной деятельности предприятия. Планирование может осуществляться на календарный год, календарный месяц, неделю, а также на иной определённый срок, обусловленный проведением важных мероприятий (работ) по видам деятельности предприятия, если они связаны с вопросами конфиденциального характера. Планы мероприятий, разрабатываемые на срок более одного календарного года, относятся, как правило, к стратегическому планированию, остальные планы решают тактические задачи.

В целях эффективного решения задач по защите конфиденциальной информации в рамках наиболее важных и масштабных работ, а также в ходе реализации на предприятии федеральных целевых, государственных, ведомственных и других программ могут разрабатываться отдельные планы, носящие характер программно-целевого планирования. Такими программами могут быть реконструкция предприятия, внедрение новых технологий, в том числе информационных, и т.п.

Планы мероприятий по защите информации относятся к документам с ограниченным доступом, учитываются и хранятся в службе безопасности (режимно-секретном подразделении) предприятия в порядке, установленном для документов соответствующей степени конфиденциальности (секретности).

Разработка планирующих документов по защите информации на предприятии осуществляется службой безопасности (режимно-секретным подразделением) в тесном взаимодействии с подразделениями (отдельными должностными лицами), в ведении которых находятся задачи, непосредственно касающиеся вопросов защиты информации (подразделение противодействия иностранным техническим разведкам, служба охраны, кадровый орган и др.). Кроме того, при подготовке планов учитываются предложения структурных подразделений предприятия, занимающихся производственной (финансово-хозяйственной) деятельностью или её обеспечением.

От полноты и качества разработки организационно-планирующих документов в полной мере зависит эффективность проведения мероприятий, направленных на исключение утечки конфиденциальной информации, утрат её носителей, а также возникновения предпосылок подобных происшествий.

9.2. СТРУКТУРА И ОСНОВНОЕ СОДЕРЖАНИЕ ПЛАНА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Основным организационно-планирующим документом предприятия является План мероприятий по защите конфиденциальной информации на календарный год. Данный план наиболее полно и всесторонне отражает мероприятия по защите информации, предполагаемые к проведению в ходе повседневной деятельности предприятия в течение календарного года. При подготовке плана учитываются вновь принятые (подписанные, утверждённые) нормативные правовые акты и методические документы по защите конфиденциальной информации, действующие приказы и текущие указания вышестоящих органов государственной власти и организаций (при наличии ведомственной принадлежности или иной подчинённости).

План мероприятий по защите конфиденциальной информации на предприятии на календарный год утверждается руководителем предприятия до начала календарного года, на который он разработан. При необходимости план согласовывается с соответствующим органом безопасности. Утверждённый план под расписку доводится до сведения заместителей руководителя предприятия, руководителей структурных подразделе-

ний и отдельных должностных лиц, ответственных за проведение указанных в плане мероприятий.

Типовой план мероприятий по защите конфиденциальной информации на календарный год содержит следующие основные разделы:

1. Организаторская работа руководства предприятия – разработка организационно-планирующих документов в ходе повседневной деятельности предприятия и при выполнении предприятием всех видов работ; представляемые в вышестоящий орган государственной власти или в вышестоящую организацию доклады и донесения о состоянии защиты информации; подготовка и издание приказов руководителя предприятия по различным вопросам в сфере защиты конфиденциальной информации; переработка и уточнение должностных обязанностей сотрудников и др.

2. Подготовка персонала по вопросам защиты информации – организация и проведение занятий со всеми категориями сотрудников предприятия с учётом специфики выполняемой ими работы; изучение положений нормативно-методических документов в области защиты информации и при необходимости доведение их требований до сведения сотрудников под расписку; принятие зачётов и проведение занятий с вновь прибывшими или назначенными на должность сотрудниками; мероприятия по обучению сотрудников предприятия в образовательных учреждениях высшего, среднего и дополнительного профессионального образования.

3. Контроль защиты информации и наличия носителей конфиденциальной информации – организация и проведение всех видов проверок состояния защиты информации и наличия носителей конфиденциальной информации. Особое внимание уделяется планированию проводимых по окончании календарного года мероприятий по проверке наличия носителей информации комиссией предприятия. Для предприятий, работающих со сведениями, составляющими государственную тайну, проведение проверок наличия носителей этих сведений планируется в соответствии со сроками, определёнными в нормативных правовых актах по обеспечению режима секретности. При наличии у предприятия подчинённых организаций, филиалов и представительств планируются проверки состояния защиты информации в этих организациях комиссиями головного предприятия.

4. Допуск и доступ персонала к конфиденциальной информации и её носителям – мероприятия, касающиеся разработки, переработки и согласования номенклатуры должностей работников предприятия, подлежащих оформлению на допуск к сведениям, составляющим государственную тайну; вопросы оформления и переоформления материалов на допуск к государственной тайне сотрудников предприятия, в том числе контрактов, трудовых договоров и карточек о допуске; разработка и переработка списков лиц, допускаемых к конфиденциальной информации, а также лиц,

допускаемых к конкретным материалам проводимых работ; мероприятия, направленные на разграничение доступа к носителям конфиденциальной информации в зависимости от степени их секретности или конфиденциальности, а также в зависимости от тематики проводимых предприятием работ.

5. При необходимости отдельным пунктом отражаются вопросы организации учёта осведомлённости лиц в сведениях особой важности и совершенно секретных сведениях, подготовки соответствующих заключений.

6. Организация и ведение конфиденциального делопроизводства – мероприятия, непосредственно касающиеся деятельности службы безопасности или режимно-секретного подразделения предприятия, а также специально создаваемых на предприятии комиссий по отбору конфиденциальных документов и материалов для уничтожения, пересмотру степени секретности или конфиденциальности материалов, инструктажу лиц, убывающих с носителями конфиденциальной информации за пределы предприятия; вопросы учёта, хранения, размножения и уничтожения носителей конфиденциальной информации, порядок работы с ними персонала предприятия.

7. Защита информации при осуществлении рекламной и публицистической деятельности – мероприятия, связанные с работой экспертной комиссии по принятию решений о возможности публикации научных материалов, информации о деятельности предприятия, использования этих материалов при проведении рекламных акций; мероприятия, осуществляемые при подготовке материалов к открытому опубликованию.

8. Защита информации при использовании технических средств – организационные мероприятия по подготовке и вводу в эксплуатацию объектов информатизации, обрабатывающих информацию с ограниченным доступом, по технической защите информации, защите информации от несанкционированного доступа и от утечки по техническим каналам; работа должностных лиц по противодействию иностранным техническим разведкам, предотвращению утечки информации при использовании средств открытой связи – например факсимильной, телеграфной, голосовой, телефонной.

9. Защита информации в ходе осуществления международного сотрудничества – мероприятия по защите информации при подготовке и реализации международных договоров и иных документов, приёме иностранных делегаций на предприятии. Мероприятия предусматриваются с учётом распределения функций по защите информации между структурными подразделениями предприятия (отделами, службами) и должностными лицами.

10. Выезд за границу сотрудников, допущенных к конфиденциальной информации, – для предприятий, работающих со сведениями, составляю-

щими государственную тайну, планирование мероприятия в данном разделе осуществляется в строгом соответствии с Федеральным законом «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию», Законом Российской Федерации «О государственной тайне» и иными нормативными правовыми актами Российской Федерации. Планируемые мероприятия не должны быть направлены на ограничение права сотрудников предприятия, допущенных к конфиденциальной информации (за исключением сведений особой важности и совершенно секретных сведений), на выезд из Российской Федерации.

Защита информации при выполнении совместных и других работ – мероприятия, направленные на исключение утечки конфиденциальной информации при участии предприятия в выполнении совместных и других работ, предусмотренных уставом предприятия; порядок и условия отражения в договорах, заключаемых с заказчиками или исполнителями работ, вопросов защиты информации, содержание соответствующих пунктов указанных договоров; мероприятия по защите государственной тайны в ходе деятельности конкурсных комиссий по выбору исполнителей работ; при участии предприятия в выполнении работ в рамках государственного оборонного заказа – особенности проведения этих работ.

Для совместных работ, в которых предприятие выступает в роли заказчика или головного исполнителя, предусматриваются мероприятия по контролю эффективности защиты исполнителями этих работ конфиденциальной информации, передаваемой им предприятием в качестве исходных данных. При выполнении предприятием работ с использованием сведений, составляющих государственную тайну, в данном разделе плана предусматриваются мероприятия, определённые ст. 17 Закона Российской Федерации «О государственной тайне» (включение в договоры на проведение работ положений, содержащих меры ответственности заказчиков, головных исполнителей и исполнителей работ за несоблюдение установленных требований и т.д.).

11. Защита информации в чрезвычайных ситуациях – порядок формирования, задачи и основные направления деятельности нештатного подразделения предприятия – специальной комиссии, создаваемой приказом руководителя предприятия в целях выработки мер по предупреждению чрезвычайных ситуаций на предприятии, а также мер по защите информации при возникновении чрезвычайных ситуаций; практические меры, направленные на недопущение нанесения ущерба информационной безопасности предприятия вследствие возникновения чрезвычайной ситуаций, в том числе на предотвращение утечки защищаемой информации, утраты, хищения или уничтожения носителей конфиденциальной информации; анализ возможных угроз и различных факторов, приводящих к возникновению на предприятии чрезвычайных ситуаций. Особое вни-

мание уделяется вопросам координации действий всех структурных подразделений, участвующих в решении задач защиты информации.

При планировании мероприятий по защите информации учитываются все возможные виды и способы проявления чрезвычайных ситуаций, мероприятия по защите информации при возникновении чрезвычайных ситуаций отражаются в соответствующих планах работы предприятия (его структурных подразделений) на календарный месяц. В данном разделе плана (либо в отдельном приложении к плану) указываются также:

– фамилия, имя, отчество, домашний адрес и контактные телефоны (в том числе мобильной связи) каждого сотрудника, принимающего участие в ликвидации последствий чрезвычайной ситуации на объектах предприятия;

– очерёдность и порядок вызова (оповещения) всех сотрудников, участвующих в выполнении работ по ликвидации последствий чрезвычайной ситуации, в зависимости от её вида, сроки прибытия этих сотрудников на объекты предприятия;

– обязанности каждого сотрудника предприятия и последовательность выполнения им мероприятий (работ) в соответствии с конкретным планом действий;

– перечень сил и средств (в том числе транспортных средств и средств связи), привлекаемых к решению задач ликвидации последствий чрезвычайных ситуаций;

– места стоянки и маршруты движения транспортных средств, эвакуирующих носители конфиденциальной информации (в том числе крупногабаритные);

– маршруты эвакуации носителей конфиденциальной информации, места их сосредоточения, способы и порядок охраны эвакуированных носителей (крупногабаритных изделий), привлекаемые для охраны силы и средства (в том числе штатных подразделений охраны).

12. Пропускной режим и охрана объектов предприятия – организационные мероприятия по созданию и совершенствованию системы пропускного режима и охраны, такие как подготовка приказов о вводе в действие или о выводе из действия всех видов пропусков, о назначении ответственных должностных лиц, разработка и переработка инструкций и положений, мероприятия по материально-техническому обеспечению, установке и эксплуатации технических средств охраны и др.

13. Аналитическая работа на предприятии – все виды обзоров и отчётов о состоянии дел в области защиты информации на предприятии, оформляемых для руководства предприятия, а также для руководителей вышестоящих органов государственной власти или вышестоящих организаций; мероприятия по формированию материалов, содержащих итоги работы предприятия и его структурных подразделений по защите инфор-

мации, для изучения всеми сотрудниками предприятия. Особое место в разделе занимают аналитические отчёты по итогам календарного месяца и календарного года, которые готовит служба безопасности (режимно-секретное подразделение) предприятия.

При необходимости включения в план иных мероприятий, не вошедших в перечисленные разделы, они отражаются в отдельном разделе плана («Другие мероприятия»).

Особое внимание при разработке и реализации плана мероприятий уделяется роли руководителей структурных подразделений предприятия как должностных лиц, ответственных за обеспечение защиты информации в непосредственно подчинённых им подразделениях.

Контроль за выполнением конкретных мероприятий, включённых в данный план, осуществляется руководителем предприятия и его заместителем, в ведении которого находятся вопросы защиты конфиденциальной информации. Служба безопасности (режимно-секретное подразделение) предприятия осуществляет текущий контроль за практической реализацией включённых в план мероприятий и информирует об их выполнении указанных должностных лиц.

10. ОРГАНИЗАЦИЯ АНАЛИТИЧЕСКОЙ РАБОТЫ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

10.1. ОСНОВНЫЕ НАПРАВЛЕНИЯ АНАЛИТИЧЕСКОЙ РАБОТЫ. ФУНКЦИИ АНАЛИТИЧЕСКОГО ПОДРАЗДЕЛЕНИЯ

Анализ состояния защиты информации – это комплексное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты информации, в том числе данных о состоянии работы по выявлению возможных каналов утечки информации, о причинах и обстоятельствах, способствующих утечке и нарушениям режима секретности (конфиденциальности) в ходе повседневной деятельности предприятия.

Основное предназначение аналитической работы – выработка эффективных мер, предложений и рекомендаций руководству предприятия, направленных на недопущение утечки конфиденциальной информации о деятельности предприятия и проводимых работах. Аналитическая работа должна включать элементы прогнозирования возможных действий противника по получению важной защищаемой информации.

Основные направления аналитической работы на предприятии следующие:

- анализ объекта защиты;
- анализ внутренних и внешних угроз информационной безопасности предприятия;
- анализ возможных каналов несанкционированного доступа к информации;
- анализ системы комплексной безопасности объектов;
- анализ имеющих место нарушений режима конфиденциальности информации;
- анализ предпосылок к разглашению информации, а также к утрате носителей конфиденциальной информации.

Функции анализа на предприятии возлагаются на специально создаваемое в его структуре аналитическое подразделение, которое комплектуется квалифицированными специалистами в области защиты информации.

Вместе с тем данные специалисты должны в полной мере владеть информацией по всем направлениям деятельности предприятия: знать виды, характер и последовательность выполнения производственных работ, взаимодействующие организации, специфику деятельности структурных подразделений предприятия и т.д. Как правило, аналитическое подразделение включается в состав службы безопасности предприятия.

Аналитическое подразделение должно обеспечивать руководство предприятия достоверной и аналитически обработанной информацией,

необходимой для принятия эффективных управленческих решений по всем направлениям защиты информации. Основными функциями аналитического подразделения являются:

- обеспечение своевременного поступления достоверных и всесторонних сведений по проблемам защиты информации;
- учёт, обобщение и постоянный анализ материалов о состоянии дел в системе защиты информации предприятия (его филиалов и представительств);
- анализ возможных угроз защите информации, моделирование реального сценария возможных действий конкурентов (злоумышленников), затрагивающих интересы предприятия;
- обеспечение эффективности работы по анализу имеющейся информации, исключение дублирования при её сборе, обработке и распространении;
- мониторинг ситуации на рынке продукции, товаров и услуг, а также во внешней среде в целях выявления событий и фактов, которые могут иметь значение для деятельности предприятия;
- обеспечение безопасности собственных информационных ресурсов, ограничение доступа сотрудников предприятия к аналитической информации;
- подготовка выводов и предложений, направленных на повышение эффективности планируемых и принимаемых мер по защите информации, а также уточнение (корректировку) организационно-планирующих документов предприятия и его структурных подразделений;
- выработка рекомендаций по внесению изменений и дополнений в методические документы, регламентирующие алгоритм действий сотрудников предприятия по защите информации (стандарты предприятия).

Наличие постоянной аналитической работы, её характер и результаты определяют необходимость создания системы, основы её организации, структуру и содержание системы комплексной защиты информации, требования к её эффективности и направления её развития и совершенствования. Анализ состояния системы защиты информации существенно влияет на количество, состав и структуру подразделений предприятия, непосредственно решающих задачи обеспечения ИБ (служба безопасности предприятия, служба охраны, режимно-секретное подразделение и др.). От эффективности и качества ведения на предприятии аналитической работы в полной мере зависит состояние защищённости информационных ресурсов предприятия, отнесённых к категории охраняемых, а также своевременность и обоснованность принятия мер по исключению утечки конфиденциальной информации и утрат носителей информации. Эффективность аналитической работы и её результаты служат основой для принятия руководством предприятия управленческих решений по вопросам

организации защиты информации. С учётом результатов аналитической работы могут вырабатываться следующие основные меры:

- уточнение (доработка) планов работы предприятия по защите информации, включение в них дополнительных мероприятий;
- уточнение распределения задач и функций между структурными подразделениями предприятия;
- переработка (уточнение) должностных (функциональных) обязанностей сотрудников предприятия, в том числе руководящего звена, совершенствование систем пропускного и внутриобъектового режимов;
- ограничение круга лиц, допускаемых к конфиденциальной информации по различным направлениям деятельности предприятия;
- пересмотр степени конфиденциальности сведений и их носителей;
- усиление системы охраны предприятия и его объектов, применение особых мер защиты информации на отдельных объектах (в служебных помещениях);
- принятие решений об ограничении публикаций в открытой печати, использование в рекламной и издательской деятельности отдельных материалов (материалов по отдельным темам), доступе командированных лиц, об исключении рассмотрения этих материалов на конференциях, семинарах, встречах и т.д.

Ведение эффективной аналитической работы возможно лишь при наличии необходимой информации. Для её получения нужна чётко сформулированная цель, определяющая конкретные источники информации. Аналитическая работа на предприятии должна вестись последовательно и непрерывно, представлять собой в полной мере целостное исследование.

10.2. ОСНОВНЫЕ ЭТАПЫ АНАЛИТИЧЕСКОЙ РАБОТЫ

В аналитической работе можно выделить следующие основные этапы:

- формулирование целей аналитической работы, разработка программы исследований, формулирование предварительных гипотез (результатов аналитической работы);
- отбор и анализ источников информации, сбор и обобщение информации;
- полноценный анализ имеющейся информации и подготовка выводов.

Основная форма ведения аналитической работы – аналитические исследования.

Проведение аналитических исследований требует чёткой организации процесса, оценки имеющихся ресурсов для выполнения исследований и достижения необходимого результата. Итогом исследования должны быть выводы, предложения и рекомендации по совершенствованию системы защиты информации.

На первом этапе аналитического исследования формулируются цели и задачи исследования, разрабатывается программа исследования, которая составляет научную основу сбора, обобщения, обработки и анализа всей полученной информации. Типовая программа исследований включает следующие основные разделы:

- цели и задачи аналитического исследования;
- предметы и объекты исследования;
- сроки (период) проведения аналитического исследования;
- методики проведения исследования;
- ожидаемые результаты и предполагаемые выводы.

При формулировании целей и задач исследования нужно учитывать, кто является его организатором и непосредственным исполнителем, какие силы и средства могут быть задействованы для его проведения, какие будут использоваться источники информации, способы и методы её сбора, обработки и анализа, какие существуют возможности для реализации предложений и рекомендаций, которые будут выработаны в ходе исследований.

В зависимости от поставленных целей и задач определяются конкретные методы и технологии исследования, а также процедуры сбора и обработки информации.

Наиболее типичны следующие задачи аналитического исследования:

- получение данных о состоянии системы защиты информации на предприятии (его конкретных объектах, в филиалах, представительствах);
- выявление возможных каналов утечки информации, подлежащей защите;
- определение обстоятельств, причин и факторов, способствующих возникновению каналов утечки и созданию предпосылок для утечки информации;
- подготовка для руководства предприятия (филиала, представительства) и его структурных подразделений конкретных рекомендаций по закрытию выявленных каналов утечки.

Под объектом исследования понимается всё то, что изучается и анализируется в ходе исследования. Предмет исследования – та сторона объекта, которая непосредственно подлежит изучению в ходе аналитического исследования.

Особое значение на первом этапе аналитической работы имеет формулирование предварительных гипотез (версий). Предварительные гипотезы должны объяснить роль и место выводов аналитических исследований в логической последовательности происходящих событий в сфере защиты охраняемой информации.

Построение предварительных гипотез проводится в следующем порядке. Сначала формируется полный список сведений, которые предпола-

гается исследовать (проанализировать). Вошедшие в список сведения систематизируются и располагаются по степени важности.

Далее из всего объёма информации выделяется группа наиболее значимых сведений, роль которых особенно очевидна в ситуации, подлежащей анализу и оценке. Выбранные сведения классифицируются по актуальности, способу получения и степени достоверности источника. Наиболее актуальные сведения анализируются в первую очередь.

Затем проводится выбор предварительных гипотез, объясняющих проявления тех или иных событий (появление тех или иных сведений). Причём в отношении одного события осуществляется проверка нескольких гипотез (версий). При последовательной проверке гипотез особое внимание уделяется наиболее реальным. Эти гипотезы фиксируются. Наименее реальные гипотезы отклоняются.

Таким образом, последовательно выбираются и формулируются наиболее вероятные предположения, объясняющие появление тех или иных конкретных событий (возникновение сведений). Возможные противоречия в полученных выводах о предполагаемых версиях происходящих событий устраняются путём всесторонней последовательной проверки реальности гипотез.

Результатом работы по формулированию предварительных гипотез является выбор версии, которая наиболее точно по сравнению с другими версиями объясняет причину возникновения конкретной ситуации, связанной с появлением возможного канала утечки конфиденциальной информации, и характеризует состояние системы защиты информации, в том числе – действия соответствующих должностных лиц, качество выполнения мероприятий и т.д.

На втором этапе проводится отбор и анализ источников информации, сбор и обобщение данных в целях выявления канала несанкционированного доступа к сведениям конфиденциального характера, исключения возможности возникновения такого канала.

Для этого осуществляется постоянный контроль объектов защиты (информационных ресурсов), а также степени защищённости обрабатываемой (циркулирующей) в них информации, проводится анализ данных, получаемых из различных источников.

Для решения конкретной задачи аналитического исследования в рамках второго этапа из всех имеющихся в распоряжении аналитического подразделения источников информации отбираются те, из которых поступает информация, наиболее близкая к исследуемым проблемам, и в то же время достаточно достоверная.

Аналитическое исследование источников информации предусматривает проведение следующих основных мероприятий:

- формирование исчерпывающего перечня источников конфиденциальной информации на предприятии;

- формирование и своевременное уточнение перечня и состава конфиденциальной информации, реально циркулирующей (обрабатываемой) на объектах предприятия, с указанием конкретных носителей, на которых она хранится;
- организация и ведение учёта осведомлённости сотрудников предприятия в конфиденциальной информации, накопление данных об их ознакомлении с конкретными сведениями конфиденциального характера с указанием носителей этих сведений;
- изучение и оценка соответствия степени конфиденциальности, присвоенной информации, реальной ценности этой информации;
- изучение внутренних и внешних угроз каждому имеющемуся на предприятии источнику конфиденциальной информации;
- выявление предприятий, заинтересованных в получении конфиденциальной информации (фирм-конкурентов), а также отдельных лиц-злоумышленников и их систематизация (классификация);
- анализ полноты и качества мер по защите конфиденциальной информации, принимаемых (принятых) в конкретных ситуациях. Учёт и анализ попыток представителей фирм-конкурентов, а также других злоумышленников получить конфиденциальную информацию;
- учёт и анализ контактов сотрудников предприятия с представителями фирм-конкурентов вне зависимости от того, касались ли они вопросов конфиденциального характера или нет.

В ходе изучения и исследования источников информации производится их оценка с точки зрения надёжности и достоверности получаемой из них информации. Оценка источников информации осуществляется методом ранжирования (классификации) самих источников, поступающей из них информации и способов её получения. В большинстве случаев может использоваться система экспертной оценки (непосредственно аналитиком) надёжности и достоверности полученных данных. Уровень подготовки и практические навыки позволяют сотруднику аналитического подразделения наиболее точно оценить собственно информацию, её источник и способ её получения.

При проведении оценки указанных элементов, как правило, используются следующие критерии:

1. Оценка источника:
- надёжный источник;
- обычно надёжный источник;
- довольно надёжный источник;
- не всегда надёжный источник;
- ненадёжный источник;
- источник неустановленной надёжности.

2. Оценка полученной информации:
- информация, подтверждённая другими фактами;

- информация, подтверждённая другими источниками;
- информация, с высокой степенью вероятности соответствующая действительности;
- информация, возможно соответствующая действительности;
- сомнительная информация;
- неправдоподобная информация;
- информация, установить (подтвердить) достоверность которой не представляется возможным.

3. Оценка способа получения информации источником:

- информация получена источником самостоятельно;
- информация получена источником из другого постоянного источника информации (например, открытого источника);
- информация получена источником из другого «разового» источника (например, в ходе переговоров, неформального общения).

В ходе оценки достоверности информации и её источника необходимо учитывать возможность преднамеренной дезинформации, а также получения непреднамеренно искажённой информации. В обоих случаях необходимо проведение дополнительной проверки и более подробного всестороннего анализа полученной информации для принятия решения о её использовании в ходе аналитических исследований.

С учётом результатов оценки полученной информации, а также источников и способов её получения осуществляются сбор и обобщение (систематизация) необходимых для проведения полноценного анализа сведений.

В ходе *третьего этапа* аналитической работы проводится полноценный анализ полученной информации и на основе его результатов – всесторонний анализ состояния системы защиты информации, вырабатываются эффективные меры по её совершенствованию. На этом этапе оформляются результаты аналитических исследований, готовятся выводы, рекомендации и предложения в области защиты охраняемой информации. Анализ состояния системы защиты информации включает изучение возможных каналов утечки информации, оценку эффективности мер по их закрытию, оценку действий персонала предприятия по решению задач в области защиты информации, определение основных направлений деятельности по защите информации.

10.3. СОДЕРЖАНИЕ И ОСНОВНЫЕ ВИДЫ АНАЛИТИЧЕСКИХ ОТЧЁТОВ

Основной формой представления результатов аналитических исследований является аналитический отчёт. Отчёты могут оформляться в письменном виде, также они могут быть представлены в устной форме,

сопровождаться графиками, диаграммами, рисунками, таблицами, поясняющими или отражающими результаты проведённой работы.

Основные разделы аналитического отчёта следующие:

- содержание аналитического исследования (цели и задачи аналитического исследования, пути решения поставленных задач, вопросы, подлежащие анализу и оценке; предполагаемые результаты исследования);
- источники информации, степень достоверности полученной информации (оценки полученной информации, источников и способов её получения, результаты анализа степени достоверности полученной с использованием этих источников аналитической информации);
- обобщение полученной информации (алгоритм сбора и обобщения необходимой для проведения полноценного анализа информации – из всего объёма полученной и обработанной информации выделяются наиболее значимые факты);
- основные и альтернативные версии или гипотезы (мотивированное деление версий, объясняющих или характеризующих исследуемые события и факты, на основную и дополнительные или альтернативные);
- недостающая информация (дополнительная информация, необходимая для подтверждения основной версии, её источники и способы её получения);
- заключение, выводы (результаты анализа и оценки поставленных вопросов, выводы о степени важности полученной и обработанной информации, значение этой информации для принятия конкретных решений в области защиты конфиденциальной информации, взаимосвязь результатов данного аналитического исследования с другими направлениями аналитической работы в сфере защиты информации, возможные угрозы защищаемой информации, а также возможные последствия воздействия негативных факторов);
- предложения и рекомендации по совершенствованию работы в области зашиты информации (конкретные предложения и рекомендации руководству предприятия и руководителям структурных подразделений по совершенствованию работы в области защиты конфиденциальной информации; выработанные на основе проведённого анализа полученной информации, а также различных событий и фактов конкретные меры, принятие которых необходимо для закрытия возможных каналов утечки информации и предотвращения потенциальных угроз защищаемой информации).

В отдельных случаях на основе результатов проведения более глубокого анализа состояния системы защиты информации вырабатываются алгоритм и способы действий персонала предприятия в конкретных ситуациях.

В зависимости от предназначения используются следующие основные виды аналитических отчётов:

- оперативный (тактический) отчёт;
- перспективный (стратегический) отчёт;
- периодический отчёт.

Оперативные (тактические) отчёты отражают результаты аналитических исследований, проводимых для подготовки и принятия какого-либо оперативного (экстренного) решения по вопросу кратковременного (срочного) характера. В ходе проведения таких исследований анализу и оценке подвергается информация, как правило, небольшого объёма.

Перспективные (стратегические) отчёты содержат информацию, более полную по содержанию. Анализ этой информации не ограничен по сроку (времени) его проведения. В такие отчёты, как правило, включается информация, содержащая более полный анализ предпосылок конкретных ситуаций, фактов, событий. В отчётах излагаются прогнозы и перспективы развития этих ситуаций. Отчёты этого вида соответствуют постоянным направлениям аналитических исследований.

Периодические отчёты предназначены для анализа состояния системы защиты информации (отдельных направлений защиты информации) в соответствии с разработанным и утверждённым руководством предприятия графиком. Эти отчёты не зависят от происходящих событий (возникновения различных ситуаций), связанных с защитой информации. Такие отчёты готовятся по проблемам (направлениям), являющимся объектами постоянного внимания со стороны службы безопасности предприятия (его аналитического подразделения).

К составлению отчётов, независимо от формы их представления, предъявляются общие требования, такие как наличие глубокого анализа событий (фактов, полученной информации), простота, чёткость и грамотность изложения материала, логичность приводимых рассуждений и выводов, соответствие отчётов установленной форме.

Одно из наиболее важных требований, предъявляемых к отчётам, заключается в том, что их содержание и уровень подготовки аналитического материала должны отвечать запросам конкретных потребителей аналитической информации – руководителей структурных подразделений или отдельных сотрудников предприятия.

10.4. КЛАССИФИКАЦИЯ МЕТОДОВ АНАЛИЗА ИНФОРМАЦИИ

Полнота и качество проведения аналитических исследований, достоверность полученных результатов и эффективность выработанных предложений и рекомендаций в полной мере зависят от тех методов анализа информации, которые были выбраны и использовались сотрудниками

аналитического подразделения непосредственно в ходе проведения исследований.

Применяемые в ходе аналитических исследований методы анализа информации делятся на три группы:

1) общенаучные (качественные);
2) количественные ;
3) частнонаучные .

Основные методы анализа, относящиеся к первой группе, включают метод выдвижения гипотез, метод интуиции, метод наблюдения, метод сравнения, метод эксперимента.

Из количественных методов наиболее распространён метод статистических исследований.

К третьей группе относятся методы письменного и устного опроса, метод индивидуальной беседы и метод экспертной оценки.

Метод выдвижения гипотез состоит в процедуре отделения известного от неизвестного и вычленения в неизвестном отдельных, наиболее важных элементов и фактов (событий).

Метод интуиции заключается в использовании аналитиком своей способности к непосредственному постижению истины (достижению требуемого результата) без предварительного логического рассуждения. Во многом этот метод основывается на личном опыте аналитика.

Метод наблюдения заключается в непосредственном исследовании (обследовании) конкретного объекта (источника информации, события, действия, факта), в самостоятельном описании аналитиком каких-либо фактов (событий, процессов), а также их логических связей в течение определённого времени.

Цель метода сравнения состоит в более глубоком изучении процессов (событий), происходящих на предприятии и имеющих отношение к вопросам защиты охраняемой информации. Сравниваются различные факторы, обусловливающие причины и обстоятельства, приводящие к утечке конфиденциальной информации или к возникновению предпосылок к её утечке. При использовании метода сравнения в обязательном порядке соблюдаются следующие основные условия: сравниваемые объекты (действия, явления, события) должны быть сопоставимы по своим качественным особенностям; сравнение должно определить не только элементы сходства, но и элементы различия между исследуемыми объектами.

Метод эксперимента используется для проверки результатов деятельности по конкретному направлению защиты информации или для поиска новых решений, совершенствования системы её защиты.

Роль количественных методов анализа заключается в информационном, статистическом обеспечении качественных методов. Наиболее характерен метод статистических исследований, который заключается

в проведении количественного анализа отдельных сторон исследуемого явления (факта, события). В ходе этого анализа накапливаются цифровые данные о состоянии и динамике нарушений режима конфиденциальности (секретности) в процессе проводимых работ, об эффективности решения службой безопасности (режимно-секретным подразделением) задач по их недопущению, о тенденциях развития ситуации в области информационной безопасности и т.д.

Методы письменного и устного опроса заключаются в получении путём анкетирования (или иным способом) необходимой информации от сотрудников предприятия, руководителей подразделений, а также лиц, допускающих нарушения установленного режима секретности (конфиденциальности информации). При этом в анкете указываются несколько возможных вариантов ответов на каждый поставленный вопрос.

Метод индивидуальной беседы отличает от метода письменного и устного опроса необходимость личного общения с сотрудником предприятия. Использование этого метода позволяет в динамично развивающейся беседе получить конкретную информацию в зависимости от целей аналитического исследования.

Метод экспертной оценки включает учёт и анализ различных мнений по определённому кругу вопросов, излагаемых специалистами в той или иной области деятельности предприятия, связанной с конфиденциальной информацией.

Выбор конкретных методов анализа при проведении аналитических исследований в области защиты конфиденциальной информации зависит от целей и задач исследований, а также от специфики деятельности предприятия, состава и структуры службы безопасности и её аналитического подразделения.

ЗАКЛЮЧЕНИЕ

Защита информации представляет в настоящее время одно из ведущих направлений обеспечения безопасности государства, общества и отдельной личности. Проблемы различных аспектов безопасности становятся всё более актуальными с дальнейшим развитием информационно-коммуникационных технологий. Последствия от нарушений информационной безопасности могут выразиться колоссальной суммой в денежном выражении. Именно это определяет особое внимание к вопросам изучения методов организации защиты информации, первостепенной составляющей в триаде комплексного обеспечения информационной безопасности, наряду с правовыми и инженерно-техническими методами.

Содержание предлагаемого учебного пособия отражает основные направления деятельности по организации защиты информации на предприятиях, организациях и учреждениях Российской Федерации. Организационное обеспечение информационной безопасности включает в себя работу по обеспечению выверенной кадровой политики, распределения ответственности за назначенные участки работ, регламентацию всех направлений защиты информации, лицензирование и сертификацию в сфере информационных технологий, обеспечение режима секретности при делопроизводстве и деятельности предприятия, организацию внутриобъектового режима и охрану объектов предприятия.

Динамика развития законодательства в области информационной безопасности предполагает постоянное изменение методов и форм обеспечения информационной безопасности, в том числе непрерывно развиваются и методы организации защиты информации в соответствие с вновь принимаемыми законами РФ, указами президента РФ, постановлениями правительства РФ и т.д.

СПИСОК ЛИТЕРАТУРЫ

1. **Аверченков, В. И.** Организационная защита информации : учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Москва : Изд-во «ФЛИНТА», 2011. – 184 с.

2. **Основы** организованного обеспечения информационной безопасности объектов информатизации / С. Н. Сёмкин, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. – Москва : Изд-во «Гелиос АРВ», 2005.

3. **Основы** информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – Москва : Горячая линия – Телеком, 2006. – 544 с.

4. **Организационно-правовое** обеспечение информационной безопасности : учебное пособие / А. А. Стрельцов, В. С. Горбатов, Т. А. Полякова [и др.]; под ред. А. А. Стрельцова. – Москва : Издательский центр «Академия», 2008. – 256 с.

5. **Мельников, П. В.** Информационная безопасность и защита информации / П. В. Мельников, С. А. Клейменов, А. М. Петраков. – 6-е изд. – Издательский центр «Академия», 2012.

СОДЕРЖАНИЕ

Учебное издание

ГРОМОВ Юрий Юрьевич
ИВАНОВА Ольга Геннадьевна
МАРТЕМЬЯНОВ Юрий Федорович и др.

МЕТОДЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие

Редактор Л. В. Комбарова
Инженер по компьютерному макетированию Т. Ю. Зотова

ISBN 978-5-8265-1235-7

Подписано в печать 24.12.2013.
Формат 60×84 /16. 4,65 усл. печ. л.
Тираж 100 экз. Заказ № 550

Издательско-полиграфический центр
ФГБОУ ВПО «ТГТУ»
392000, г. Тамбов, ул. Советская, д. 106, к. 14
Тел. 8(4752) 63-81-08;
E-mail: izdatelstvo@admin.tstu.ru