МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Кафедра информационной безопасности

Составители
Е. В. Прокопенко
И. В. Чичерин

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Методические материалы

Рекомендованы учебно-методической комиссией специальности
10.05.03 Информационная безопасность автоматизированных систем
в качестве электронного издания для использования
в образовательном процессе

Кемерово 2018

Рецензенты
Стенин Д. В.– кандидат технических наук, доцент, директор ИИТМА
Сыркин И. С. – кандидат технических наук, доцент кафедры информационных и автоматизированных производственных систем

Прокопенко Евгения Викторовна
Чичерин Иван Владимирович

Техническая защита информации: методические материалы [Электронный ресурс]: для обучающийся специальности 10.05.03 Информационная безопасность автоматизированных систем очной формы обучения / сост. Е. В. Прокопенко, И. В. Чичерин; КузГТУ. – Кемерово, 2018. – Систем. требования: Pentium IV; ОЗУ 8 Мб; Windows XP; мышь. – Загл. с экрана.

1. Концепция инженерно-технической защиты информации.

2. Теоретические основы инженерно-технической защиты информации.

Системы технической защиты

Концепция инженерно-технической защиты информации определяет основные принципы, методы и средства обеспечения информационной безопасности объектов.

Она представляет собой общий замысел и принципы обеспечения информационной безопасности объекта в условиях угроз и включает в себя:

• оценку угроз;

• систему защиты информации;

• принцип построения системы защиты информации.

Инженерно-техническая защита представляет собой совокупность специальных органов, технических средств и мероприятий по их использованию для защиты конфиденциальной информации.

Эффективная техническая защита информационных ресурсов является неотъемлемой частью комплексной системы обеспечения информационной безопасности и способствует оптимизации финансовых затрат на организацию защиты информации.

Техническая защита информации предполагает комплекс мероприятий по защите информации:

- от **несанкционированного доступа** по различным каналам,

- а также **нейтрализацию специальных воздействий на нее** – уничтожения, искажения или блокирования доступа.

Цели и задачи технической защиты:

• предотвращение проникновения злоумышленника к источникам информации с целью уничтожения, хищения или изменения;

• защита носителей информации от уничтожения в результате различных природных и техногенных воздействий;

• предотвращение утечки информации по различным техническим каналам.

Принципы проектирования систем технической защиты :

• непрерывность защиты информации в пространстве и во времени, постоянная готовность и высокая степень эффективности по ликвидации угроз информационной безопасности;

• **многозональность и многорубежность** защиты, задающее размещение информации различной ценности во вложенных зонах с контролируемым уровнем безопасности;

• избирательность, заключающаяся в предотвращении угроз в первую очередь для наиболее важной информации;

• интеграция (взаимодействие) различных систем защиты информации с целью повышения эффективности многокомпонентной системы безопасности;

• создание централизованной службы безопасности в интегрированных системах.

По функциональному назначению средства инженерно-технической защиты подразделяются на следующие группы:

• инженерные средства, представляющие собой различные устройства и сооружения, противодействующие физическому проникновению злоумышленников на объекты защиты;

• аппаратные средства (измерительные приборы, устройства, программно-аппаратные комплексы и др.), предназначенные для выявления каналов утечки информации, оценки их характеристик и защиты информации;

• программные средства, программные комплексы и системы защиты информации в информационных системах различного назначения и в основных средствах обработки данных;

• криптографические средства, специальные математические и алгоритмические средства защиты компьютерной информации, передаваемой по открытым системам передачи данных и сетям связи.

В концепции инженерно-технической защиты информации кроме целей и задач системы безопасности, определяются:

- принципы ее организации и функционирования;

- правовые основы;

- виды угроз и ресурсы, подлежащие защите,

- а также **основные направления разработки системы безопасности, включая:** физическую, правовую, организационную, экономическую, инженерно-техническую, программно-математическую защиту, информационно-аналитическое обеспечение и консультативную помощь.

К целям защиты информации относятся:

- предотвращение утечки, хищения, утраты, искажения, подделки информации и предотвращение других несанкционированных негативных воздействий.

Безопасная информационная деятельность требует наличия системы ее защиты:

– комплекса организационных,

- организационно-технических

- и технических мероприятий по обнаружению, предотвращению и ликвидации возникших угроз объекту.

Создание новой системы защиты или оценка эффективности существующей системы безопасности объекта начинается с анализа возможных угроз и оценки их реального появления.

Основой для анализа является исследование объекта на:

- наличие уязвимостей в защите,

- изучение расположения и особенностей инженерных конструкций, коммуникаций и т.п.

На следующем этапе осуществляется выбор соответствующих методов и средств адекватной защиты.

При оценке вероятных угроз объекту должны учитываться:

- угрозы здоровью и безопасности персонала;

- угрозы целости и сохранности материальных ценностей и оборудования;

- безопасность информации,

- сохранность государственной или коммерческой тайны.

Для получения максимально реальной оценки угроз необходимы изучение и анализ статистических данных, связанных с попытками разведывательной деятельности на объекте в прошлом; оценка риска по каждому виду угроз; оценка ситуации на объекте и прилегающих к нему территориях на определенном интервале времени; изучение статистики по фактам разведдеятельности на подобных объектах.

Важным моментом в объективной оценке угроз и в разработке концепции защиты объекта является привлечение независимых экспертных организаций или специализированных государственных учреждений, имеющих квалифицированный персонал. В этом случае исключается субъективная оценка разведдоступности объекта и проводится квалифицированная разработка концепции защиты.

Несмотря на большое разнообразие возможных информационных угроз, проектирование защиты от каждой из них должно вписываться в комплексную систему защиты. Комплексная система защиты предусматривает надежное перекрытие всех опасных каналов утечки информации.

Эффективность системы защиты основных и вспомогательных технических средств от утечки информации по техническим каналам оценивается по различным критериям, которые определяются физической природой информационного сигнала, но чаще всего по соотношению «сигнал/шум».

Все способы защиты согласно руководящей документации делятся на две группы:

• скрытие;

• дезинформация.

К первой группе относятся:

• пассивное скрытие;

• активное скрытие;

• специальная защита.

Ко второй группе относятся:

• техническая дезинформация;

• имитация;

• легендирование.

Суть пассивного скрытия заключается в исключении или значительном затруднении обнаружения объектов, а также в ослаблении до необходимого уровня их демаскирующих признаков.

Пассивное скрытие состоит из организационных мероприятий и технических мер.

К организационным мероприятиям относятся:

• территориальное, пространственно-временное, энергетическое и частотное ограничения на функционирование объектов;

• затруднения для ведения технической разведки путем использования маскирующих свойств местности, местных предметов, времени суток;

• установление контролируемых зон в месте расположения скрываемых видовых объектов.

К техническим мерам пассивного скрытия относятся:

• снижение контрастности демаскирующих признаков скрываемых видовых объектов по отношению к фону;

• снижение уровня информационных физических полей, создаваемых функционирующим объектом;

• применение маскирующих покрытий для видовых объектов;

• камуфлирование техники;

• применение при настройке радиоэлектронной аппаратуры эквивалентов антенн, закрытых антенно-фидерных устройств, экрани-

рованных камер и сооружений, исключающих электромагнитные излучения в окружающее пространство.

Суть активного скрытия состоит главным образом в создании маскирующих шумовых помех различной физической природы техническим средствам разведки и в создании ложной обстановки по физическим полям скрываемого объекта.

Активное скрытие применяется в большинстве случаев как дополнительная мера к пассивному скрытию, когда не обеспечиваются условия снижения уровня физического поля до безопасного значения.

Спецзащита реализуется аппаратными, криптографическими и программными способами. К спецзащите относятся скремблирование телефонных переговоров, кодирование цифровой информации криптографическими методами, программные методы модификации информации.

К принципам инженерно-технической защиты информации относятся :

- надежность защиты информации;
- непрерывность защиты;
- скрытность защиты информации;
- рациональность защиты;
- многообразие способов защиты;
- комплексное применение различных способов и средств защиты;
- экономичность защиты.

Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.

Виды: семантическая и признаковая информация.

Признаковая информация.

Любая информация содержится на материальных носителях в виде значений их признаков, т. е. она отображается на носителях информации на языке признаков. Язык признаков является универсальным языком представления информации в материальном мире. Информация, отображаемая на языке признаков, называется **признаковая.**

Информация признаковая является первичной и описывает конкретный материальный объект на языке его признаков. Описание объекта содержит признаки его внешнего вида, излучаемых им полей и элементарных частиц, состава и структуры веществ, из которых состоит объект.

Источниками признаковой информации являются сами объекты. К ним в первую очередь относятся интересующие зарубежную разведку или отечественного конкурента люди, новая продукция и материалы, помещения и даже здания, в которых может находиться конфиденциальная информация.

В зависимости от вида описания объекта признаковая информация делится на информацию:

- о внешнем виде (видовых признаках),
- о его полях (признаках сигналов),
- о структуре и составе его веществ (признаках веществ).

Признаки принадлежат конкретному объекту, но их значения могут отражать как свойства самого объекта, так и результаты взаимодействия рассматриваемого объекта с другими.

Семантическая информация по отношению к признаковой является вторичной, синтезируемой второй сигнальной системой человека в результате кодирования признаков символами. Когда человек читает текст книги, его зрительный анализатор сканирует поверхность листа и выделяет видовые признаки текста, а вторая сигнальная система формирует текущие признаковые структуры символов (букв, цифр, слов) и распознает символы в результате идентификации их текущих признаковых структур с эталонными структурами. Если человек не обучен иностранному языку, то в его памяти отсутствуют эталонные признаковые структуры букв и слов иностранного языка, и он не понимает текст в книге.

Если признак привязан к конкретному объекту, то символьная (семантическая) информация абстрактна.

Сущность семантической информации не зависит от характеристик носителя.

Содержание текста, например, не зависит от качества бумаги, на которой он написан, или физических параметров другого носителя. **Семантическая информация – продукт абстрактного мышления человека и обработки данных рецепторов других живых существ. Семантическая информация**, циркулирующая в человеческом обществе, отображает создаваемые ими образы и модели с помощью символов на языках общения людей.

Языки общения включают как естественные языки национального общения, так и искусственные профессиональные языки. Любой язык включает набор символов – алфавит и правила их использования – грамматику.

Для обеспечения эффективной защиты информации необходимо знать ее свойства. Она как предмет защиты обладает рядом свойств, основные из которых следующие:

1. **Нематериальная информация** может храниться, передаваться, обрабатываться, если она содержится на материальном носителе. Так как с помощью материальных средств можно защищать только материальный объект, **то объектами защиты являются материальные носители информации.** Различают носители – источники информации, носители – переносчики информации и носители– получатели информации.

2. Информация может быть для ее для пользователя (собственника, владельца, получателя) достоверной и ложной, полезной и вредной. Информация, отражающие объективные факты, события, явления и процессы, является **достоверной,** а не соответствующая им – **ложной.** Границу между достоверной и ложной информацией часто трудно провести. Достоверная информация в процессе передачи может трансформироваться в свою противоположность. Преднамеренно создаваемая и распространяемая ложная информация называется **дезинформацией.**

3. Хотя информация нематериальная, она покупается и продается. Поэтому **информацию можно рассматривать как товар.** Полезность информации как товара характеризуется его ценой. Цена информации зависит от ее ценности, но это разные понятия.

4. Полезность (цена) информации изменяется во времени. Распространение информации и ее использование приводят к изменению ее ценности и цены. Характер изменения ценности во времени зависит от вида информации. Для научной информации эта зависимость часто имеет волнообразный вид. Информация об открытии даже новых законов или явлений природы вначале должным образом не оценивается.

5. Невозможно объективно (без учета полезности ее для потребителя, владельца, собственника) оценить количество информации. Для обеспечения эффективной защиты информации важно знать количество защищаемой информации. Однако объективно определить ее невозможно. Например, количество информации, содержащейся в книге, для разных читателей – разное. Даже один и тот же человек в разные периоды своей жизни находит в книге каждый раз что-то новое для себя. Количество информации в голове человека

можно косвенно оценить по его действиям, так как для принятия обоснованного решения необходимо больше информации.

6. Информация способна случайным образом «растекаться» в пространстве. Так как человеку присуща любознательность, переходящая у многих в любопытство, а также иногда даже трудно сдерживаемое желание поделиться с другими новостями, то при общении (взаимодействии) людей происходит выравнивание их тезаурусов. Следовательно, в организации и обществе, если не предпринимаются дополнительные усилия по поддержанию неравномерности информационной энтропии, происходит ее выравнивание, т. е. выравнивание тезаурусов разных сотрудников или членов общества. Выравнивание тезаурусов происходит путем передачи информации от тезауруса большего объема тезаурусу меньшего объема. Кроме целенаправленной (законной или незаконной) деятельности по передаче информации имеют место случайные процессы выравнивания тезаурусов владельцев, аналогично выравниванию температуры в замкнутом пространстве.

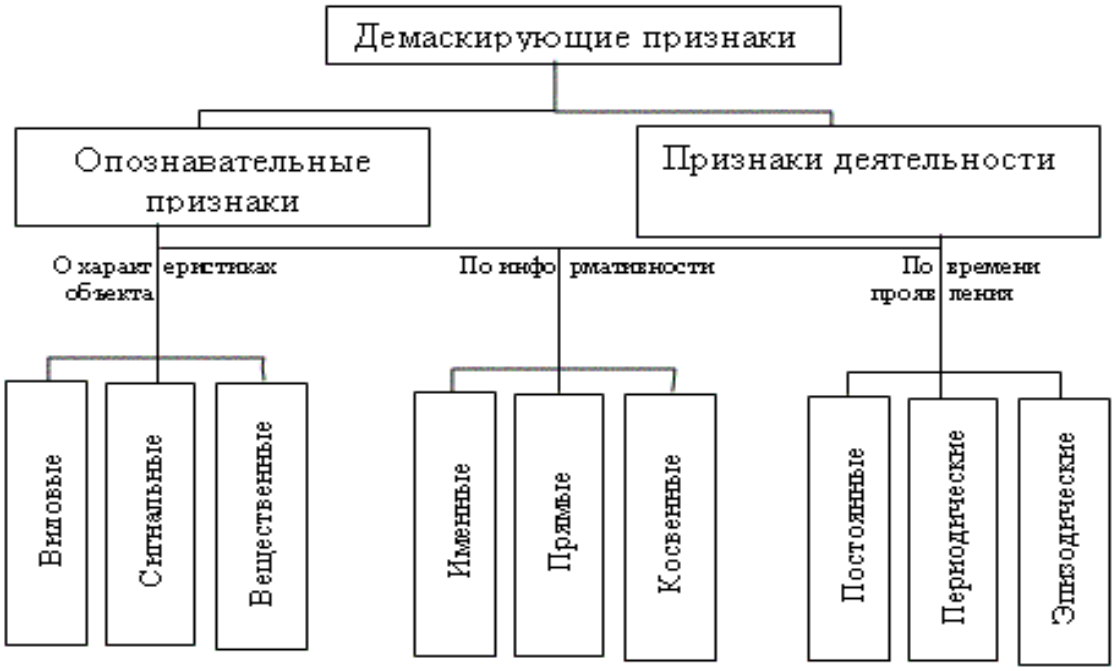
7. При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается. После снятия копии с документа на ксероксе или другим способом количество информации в нем не меняется. В результате этого несанкционированное копирование (хищение) информации может остаться незамеченным для ее владельца**,** если отсутствуют иные признаки проникновения злоумышленника к ее источнику и факта хищения. Но если при копировании происходят воздействия на информационные параметры носителя, приводящие к изменению их значений, или незначительные изменения накапливаются, то количество информации уменьшается. Ухудшается качество звука и изображения соответственно на ауд**ио-** и видеопленке из-за механического разрушения магнитного **слоя,** книжка зачитывается до дыр, блекнут яркие цвета на картинке репродукциях на стенах светлой комнаты.

Так как при каждом копировании увеличивается число ее законных и незаконных пользователей, то в соответствии е законами рынка цена снижается. Например, видеопиратство вызывает большое беспокойство у владельцев видеопродукции, так как широкое распространение пиратских копий значительно сбивает цены на рынке.

Классификация демаскирующих признаков

Признаки, позволяющие отличить один объект от другого, называются демаскирующими**.**

Классификация демаскирующих признаков



Демаскирующие признаки объекта описывают его различные состояния, характеристики и свойства.

Демаскирующие признаки объектов разделяются на **опознавательные признаки** и **признаки деятельности.**

Опознавательные признаки описывают объекты **в статическом состоянии:** его назначение, принадлежность, параметры. Признаки деятельности объектов характеризуют этапы и режимы функционирования объектов, например, этапы создания новой продукции: научные исследования, подготовка к производству, изготовление новой продукции, ее испытания и т. д.

Демаскирующие признаки характеристик объекта можно разделить на 3 группы:

- видовые признаки; (форма объекта, его размеры, детали объекта, тон, цвет и структура его поверхности и др.);

- признаки сигналов; (параметры полей и электрических сигналов, генерируемых объектом: их мощность, частоту, вид (аналоговый, импульсный), ширину спектра и т. д.);

- признаки веществ (физический и химический состав, структуру и свойства веществ материального объекта).

Таким образом совокупность демаскирующих признаков рассмотренных трех групп представляет собой модель объекта, описывающую:

- его внешний вид,
- излучаемые им поля,
- внутреннюю структуру,
- и химический состав содержащихся в нем веществ.

Важнейшим показателем признака является его информативность.

Информативность можно оценивать мерой в интервале [0-1], соответствующей значению **вероятности обнаружения объекта по конкретному признаку.**

Чем **признак более индивидуален,** т. е. принадлежит меньшему числу объектов, **тем он более информативен.**

Наиболее информативен именной признак, присущий только одному конкретному объекту.

Такими признаками являются фамилия, имя, отчество человека, папиллярный узор его пальцев, инвентарный номер прибора или образца мебели. Факты, например, о совпадении папиллярных узоров пальцев разных людей не известны.

Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых прямыми, колеблется в пределах [0-1].

Признаки, непосредственно не принадлежащие объекту, но отражающие свойства и состояние объекта, называются косвенными. Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой.

К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов.

3. Физические основы защиты информации.

4. Технические средства добывания и инженерно-технической защиты информации.

Как отмечают специалисты, до 80% информации добывается в настоящее время с использованием радиоэлектронных средств. В этих условиях повышается роль мероприятий по защите сведений составляющих государственную, военную, коммерческую тайну. В курсе лекций будут рассмотрены физические процессы которые лежат в основе построения средств защиты от съема информации.

Основная задача получения информации – добывание сведений путем обнаружения, перехвата открытых или кодированных засекреченных передач с каналов связи (ВОЛС и т.д.) связных радиостанций, пеленгование источников РС и определение их местонахождения.

Технические средства получения информации по принципу действия делятся на 2 группы:

1. Пассивные средства, которые добывают информацию благодаря приему сигналов излучаемых радиоэлектронными средствами противника (радио, радиотехническая, телевизионная).

2. Активные средства, которые используя свои собственные источники радиоизлучения получают информацию путем приема и фиксации сигналов отраженных от объектов съема информации.

Средства защиты – это препятствия для нарушителей на пути к защищаемым данным. Физические средства ЗИ выполняют:

1) охрану территорий и зданий,
2) охрану внутренних помещений,
3) охрану оборудования и наблюдение за ним,
4) контроль доступа,
5) нейтрализация излучения и наводок,
6) создание препятствий визуальному наблюдению,
7) противопожарная защита,
8) блокировка действий нарушителя,
9) системы защиты окон и дверей.

Вопрос 2. Содержание курса лекций «Физические основы защиты информации»

Курс в основном рассматривает: физические основы защиты информации от утечки по каналам, образующимся электромагнитными явлениями.

1. Физические основы механизмов, создающих утечку информации по техническим каналам, а также искажение информации.

2. Физические основы действий, направленных на защиту информации от утечки по техническим каналам и противодействующих средствам технической разведки.

3. Фундаментальные физические пределы и ограничения, определяющие потенциальные характеристики технических каналов утечки информации и мероприятий по защите от утечки по этим каналам.

4. Возможности современной техники и технологии в части достижения фундаментальных пределов в решении задач создания тех-

нических каналов утечки информации и защиты от утечки по этим каналам.

5. Количественные оценки характеристик каналов утечки информации: потенциальные и реально существующие.

6. Количественные оценки возможностей технических средств разведки.

7. Количественные оценки требуемых мер защиты от утечки информации по техническим каналам.

Основной направленностью содержания курса является количественное описание явлений, процессов и действий, выполняемых и существующих при решении задач защиты информации от утечки по техническим каналам.

Рассматриваются модели ситуаций возникновения утечки информации и производится количественное описание этих каналов с оценкой их реальности, опасности, дальности действия, требуемых мер по защите.

Рассматриваются характеристики радиоканала передачи информации. Оценивается влияние мощности источника излучения (передатчика), влияние передающей антенны, влияние приемника (с оценкой достижимости характеристик по чувствительности, избирательности и другим), влияние приемных антенн.

Рассматриваются возможности и ограничения методов защиты от утечки информации основанных на электромагнитном экранировании, на применении генераторов шума.

Рассматриваются методы обнаружения электромагнитных излучений и источников излучений с применением широкополосных индикаторов поля, узкополосных сканирующих приемников, анализаторов спектра, нелинейных локаторов.

Вопрос 3. Технические каналы утечки информации. Постановка задачи. Нормативная база. Физические основы.

Защита информации от утечки по техническим каналам – это комплекс организационных, организационно-технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

В основе утечки информации лежит неконтролируемый перенос конфиденциальной информации посредством акустических, световых, электромагнитных, радиационных и других полей и материальных объектов.

Причины и условия утечки информации при всех своих различиях имеют много общего.

Причины утечки информации связаны, как правило, с несовершенством норм по сохранению информации, а также нарушением этих норм (в том числе и несовершенных), отступлением от правил обращения с соответствующими документами, техническими средствами, образцами продукции и другими материалами, содержащими конфиденциальную информацию.

Условия включают различные факторы и обстоятельства, которые складываются в процессе научной, производственной, рекламной, издательской, отчетной, информационной и иной деятельности предприятия и создают предпосылки для утечки информации. К таким факторам и обстоятельствам могут, например, относиться:

- Недостаточное знание работниками предприятия правил защиты информации и непонимание необходимости их тщательного соблюдения;
- Использование не аттестованных технических средств обработки конфиденциальной информации;
- Слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;
- Текучесть кадров, в том числе владеющих сведениями конфиденциального характера.

Таким образом, большая часть причин и условий, создающих предпосылки и возможность утечки информации, возникает из-за недоработок руководителей предприятий и их сотрудников.

Кроме того, утечке информации способствуют:

- Стихийные бедствия (шторм, ураган, смерч, землетрясение, наводнение);
- Неблагоприятная внешняя среда (гроза, дождь, снег);
- Катастрофы (пожар, взрывы);
- Неисправности, отказы, аварии технических средств и оборудования.

Технические каналы утечки информации являются источником информации для служб, осуществляющих добывание информации с помощью технических средств. Считается, что на долю таких технических служб приходится более 50% всей добываемой информации. Поэтому проблема защиты от технической разведки имеет особую актуальность.

Характеристика технических каналов утечки информации

Под техническим каналом утечки информации понимают совокупность источника информации, линии связи (физической среды), по которой распространяется информационный сигнал, шумов, препятствующих передаче сигнала в линии связи, и технических средств перехвата информации.

Источниками информации могут быть непосредственно голосовой аппарат человека, вычислительная техника, излучатели систем звукоусиления, печатный текст, радиопередающие устройства и др.

Сигналы являются материальными носителями информации. По своей природе сигналы могут быть электрическими, электромагнитными, акустическими, оптическими и т.д.

В зависимости от природы сигналы распространяются в определенных физических средах.

Шумы сопровождают все физические процессы и присутствуют на входе средств перехвата информации.

Средства перехвата информации служат для приема и преобразования сигналов с целью получения информации.

Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации

К техническим средствам приема информации (ТСПИ), а также ее обработки, хранения и передачи относят технические средства, непосредственно обрабатывающие конфиденциальную информацию. В их число входят электронно-вычислительная техника, АТС для ведения секретных переговоров, системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

При выявлении технических каналов утечки информации ТСПИ необходимо рассматривать как систему, включающую основное оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления. Перечисленные технические средства называют основными техническими средствами.

Наряду с ТСПИ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ТСПИ и находящиеся в зоне электромагнитного и других полей со-

здаваемых ТСПИ. Такие технические средства и системы называют вспомогательными техническими средствам и системами (ВТСС). Это технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, средства и системы кондиционирования, электрификации, радиофикации, часофикации, электробытовые приборы и т. д.

В качестве канала утечки информации наибольшую опасность представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ).

Контролируема зона – территория (здание, группа помещений, помещение), на которой исключено неконтролируемое перемещение лиц и транспортных средств, не имеющих постоянного или разового допуска. В контролируемой зоне посредством проведения технических и режимных мероприятий должны быть созданы условия, предотвращающие возможность утечки из нее конфиденциальной информации. Контролируема зона определяется руководством организации, исходя из конкретной обстановки в месте расположения объекта и возможностей использования средств для съема информации.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

В зависимости от физической природы образования каналов утечки информации их можно разделить на следующие группы:

- Визуально-оптические;
- Акустические (включая акустико-преобразовательные);
- Электромагнитные (включая магнитные, электрические и параметрические [3]);
- Материально-вещественные (бумага, фото, магнитные носители, производственные отходы и др.).

Вопрос 4. Основы нормативной базы организации защиты информации в Российской федерации

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) "Об информации, информационных технологиях и о защите инфор-

мации", принят Государственной Думой 8 июля 2006 г., одобрен Советом Федерации 14 июля 2006 г.

Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом (в ред. Федерального закона от 02.07.2013 № 187-ФЗ).

В настоящем ФЗ, даны:

Статья 1

Статью 28 Арбитражного процессуального кодекса Российской Федерации (Собрание законодательства Российской Федерации, 2002, N 30, ст. 3012) дополнить словами ", за исключением дел, рассматриваемых Московским городским судом в соответствии с частью третьей статьи 26 Гражданского процессуального кодекса Российской Федерации".

Статья 2

Внести в Гражданский процессуальный кодекс Российской Федерации (Собрание законодательства Российской Федерации, 2002, № 46, ст. 4532; 2005, № 30, ст. 3104; 2006, № 1, ст. 8; 2007, № 41, ст. 4845; 2008, № 24, ст. 2798; 2009, № 14, ст. 1579; 2010, № 18, ст. 2145; № 50, ст. 6611; 2011, № 49, ст. 7066) следующие изменения:

1) статью 26 дополнить частью третьей следующего содержания:

"3. Московский городской суд рассматривает в качестве суда первой инстанции гражданские дела, которые связаны с защитой исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", и по которым им приняты предварительные обеспечительные меры в соответствии со статьей 144.1 настоящего Кодекса.";

2) часть первую статьи 140 дополнить пунктом 3.1 следующего содержания:

"3.1) возложение на ответчика и других лиц обязанности совершить определенные действия, касающиеся предмета спора о нарушении исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет";";

3) дополнить статьей 144.1 следующего содержания:

"Статья 144.1. Предварительные обеспечительные меры защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет"

1. Суд по письменному заявлению организации или гражданина вправе принять предварительные обеспечительные меры, направленные на обеспечение защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, заявителя в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", до предъявления иска. Такое заявление также может быть подано в суд посредством заполнения формы, размещенной на официальном сайте суда в информационно-телекоммуникационной сети "Интернет", и подписано квалифицированной электронной подписью в установленном федеральным законом порядке.

2. Предварительные обеспечительные меры, предусмотренные настоящей статьей, принимаются судом по правилам, предусмотренным настоящей главой, с особенностями, установленными настоящей статьей.

3. Заявление о предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", подается в Московский городской суд.

4. При подаче заявления о предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", заявитель представляет в суд документы, подтверждающие факт использования в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", объектов исключительных прав и права заявителя на данные объекты. Непредставление указанных документов в суд является основанием для вынесения определения об отказе в предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том

числе в сети "Интернет", в котором суд разъясняет право на повторную подачу указанного заявления с выполнением требований настоящей части, а также право на подачу иска в общем порядке. При подаче заявления о предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", в соответствии с настоящей статьей посредством заполнения формы, размещенной на официальном сайте Московского городского суда в информационно-телекоммуникационной сети "Интернет", документы, подтверждающие факт использования в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", объектов исключительных прав и права заявителя на указанные объекты, могут быть представлены в электронном виде.

5. О предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", суд выносит определение.

В определении устанавливается срок, не превышающий пятнадцати дней со дня вынесения определения, для подачи искового заявления по требованию, в связи с которым судом приняты меры по обеспечению имущественных интересов заявителя. Указанное определение размещается на официальном сайте Московского городского суда в информационно-телекоммуникационной сети "Интернет" не позднее следующего дня после дня вынесения указанного определения.

6. В случае принятия судом предварительных обеспечительных мер, предусмотренных настоящей статьей, исковое заявление о защите исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", подается заявителем в указанный суд.

7. Если заявителем не было подано исковое заявление в срок, установленный определением суда о предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", предварительное обеспечение отменяется тем же судом. Об отмене предварительного обеспечения выносится определение.

Определение об отмене предварительного обеспечения размещается на официальном сайте Московского городского суда в ин-

формационно-телекоммуникационной сети "Интернет" не позднее следующего дня после дня вынесения указанного определения.

Копии определения направляются заявителю, в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, и иным заинтересованным лицам не позднее следующего дня после дня вынесения определения.

8. В случае подачи заявителем искового заявления по требованию, в связи с которым судом приняты меры по предварительному обеспечению защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", эти меры действуют как меры по обеспечению иска.

9. Организация или гражданин, права и (или) законные интересы которых нарушены принятием мер по предварительному обеспечению защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", до предъявления иска вправе требовать по своему выбору от заявителя возмещения убытков в порядке, установленном статьей 146 настоящего Кодекса, если заявителем в установленный судом срок не было подано исковое заявление по требованию, в связи с которым судом были приняты указанные предварительные обеспечительные меры, или если вступившим в законную силу судебным актом в иске отказано.";

4) статью 320.1 дополнить пунктом 5 следующего содержания:

"5) апелляционной инстанцией Московского городского суда – на решения данного суда по гражданским делам, которые связаны с защитой исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", и по которым им приняты предварительные обеспечительные меры в соответствии со статьей 144.1 настоящего Кодекса.";

5) часть первую статьи 428 дополнить абзацем следующего содержания:

"Исполнительный лист по определению о предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, выдается взыскателю не позднее следующего дня после дня вынесения такого определения.";

6) статью 429 дополнить частью третьей следующего содержания:

"3. На основании определения о предварительном обеспечении защиты исключительных прав на фильмы, в том числе кинофильмы, телефильмы, в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", суд выдает исполнительный лист взыскателю, а также по ходатайству взыскателя направляет исполнительный лист в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.".

Статья 3

Внести в Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328; 2013, № 14, ст. 1658; № 23, ст. 2870) следующие изменения:

1) часть 2 статьи 1 дополнить словами ", за исключением случаев, предусмотренных настоящим Федеральным законом";

2) дополнить статьей 15.2 следующего содержания:

"Статья 15.2. Порядок ограничения доступа к информации, распространяемой с нарушением исключительных прав на фильмы, в том числе кинофильмы, телефильмы

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", фильмов, в том числе кинофильмов, телефильмов, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие фильмы или информацию, на основании вступившего в силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных

технологий и связи.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети "Интернет", указанного информационного ресурса, обслуживающего владельца сайта в сети "Интернет", на котором размещена информация, содержащая фильмы, в том числе кинофильмы, телефильмы, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания;

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении исключительных прав на фильмы, в том числе кинофильмы, телефильмы, с указанием наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети "Интернет", на котором размещена информация, содержащая фильмы, в том числе кинофильмы, телефильмы, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания, а также указателей страниц сайта в сети "Интернет", позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в соответствующей информационной системе.

3. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить незаконно размещенную информацию и (или) принять меры по ограничению доступа к ней.

4. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 2 настоящей

статьи лица уведомления о необходимости удалить незаконно размещенную информацию владелец информационного ресурса обязан удалить такую информацию. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи.

5. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 2 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 3 и 4 настоящей статьи, доменное имя сайта в сети "Интернет", его сетевой адрес, указатели страниц сайта в сети "Интернет", позволяющие идентифицировать информацию, содержащую фильмы, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, и размещенную без разрешения правообладателя или иного законного основания, а также иные сведения об этом сайте и информация направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети "Интернет", или к размещенной на нем информации.

6. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней со дня получения судебного акта об отмене ограничения доступа к информационному ресурсу, содержащему фильмы, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, уведомляет провайдера хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо и операторов связи об отмене мер по ограничению доступа к данному информационному ресурсу.

7. В течение суток с момента получения по системе взаимодействия сведений об информационном ресурсе, содержащем фильмы, в том числе кинофильмы, телефильмы, или информацию, необходимую для их получения с использованием информационно-телекоммуника-

ционных сетей, которые распространяются без разрешения правообладателя или иного законного основания, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети "Интернет", обязан ограничить доступ к такому информационному ресурсу, в том числе к сайту в сети "Интернет", или к странице сайта.

8. Порядок функционирования информационной системы взаимодействия устанавливается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. Предусмотренный настоящей статьей порядок не применяется к информации, подлежащей включению в реестр в соответствии со статьей 15.1 настоящего Федерального закона.";

3) статью 17 дополнить частью 4 следующего содержания:

"4. Провайдер хостинга и владелец сайта в сети "Интернет" не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.".

Статья 4

Внести в часть четвертую Гражданского кодекса Российской Федерации (Собрание законодательства Российской Федерации, 2006, № 52, ст. 5496; 2008, № 27, ст. 3122; 2010, № 41, ст. 5188) следующие изменения:

1) дополнить статьей 1253.1 следующего содержания:

"Статья 1253.1. Особенности ответственности информационного посредника

1. Лицо, осуществляющее передачу материала в информационно- телекоммуникационной сети, в том числе в сети "Интернет", лицо, предоставляющее возможность размещения материала или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети, лицо, предоставляющее возможность доступа к материалу в этой сети, – информационный посредник – несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, предусмотренных настоящим Кодексом, при наличии вины с учетом особенностей, установленных пунктами 2 и 3 настоящей статьи.

2. Информационный посредник, осуществляющий передачу материала в информационно-телекоммуникационной сети, не несет ответственность за нарушение интеллектуальных прав, произошедшее в результате этой передачи, при одновременном соблюдении следующих условий:

1) он не является инициатором этой передачи и не определяет получателя указанного материала;

2) он не изменяет указанный материал при оказании услуг связи, за исключением изменений, осуществляемых для обеспечения технологического процесса передачи материала;

3) он не знал и не должен был знать о том, что использование соответствующих результата интеллектуальной деятельности или средства индивидуализации лицом, инициировавшим передачу материала, содержащего соответствующие результат интеллектуальной деятельности или средство индивидуализации, является неправомерным.

3. Информационный посредник, предоставляющий возможность размещения материала в информационно-телекоммуникационной сети, не несет ответственность за нарушение интеллектуальных прав, произошедшее в результате размещения в информационно-телекоммуникационной сети материала третьим лицом или по его указанию, при одновременном соблюдении информационным посредником следующих условий:

1) он не знал и не должен был знать о том, что использование соответствующих результата интеллектуальной деятельности или средства индивидуализации, содержащихся в таком материале, является неправомерным;

2) он в случае получения в письменной форме заявления правообладателя о нарушении интеллектуальных прав с указанием страницы сайта и (или) сетевого адреса в сети "Интернет", на которых размещен такой материал, своевременно принял необходимые и достаточные меры для прекращения нарушения интеллектуальных прав. Перечень необходимых и достаточных мер и порядок их осуществления могут быть установлены законом.

4. К информационному посреднику, который в соответствии с настоящей статьей не несет ответственность за нарушение интеллектуальных прав, могут быть предъявлены требования о защите интеллектуальных прав (пункт 1 статьи 1250, пункт 1 статьи 1251, пункт 1 статьи 1252 настоящего Кодекса), не связанные с применением мер

гражданско-правовой ответственности, в том числе об удалении информации, нарушающей исключительные права, или об ограничении доступа к ней.

5. Правила настоящей статьи применяются в отношении лиц, предоставляющих возможность доступа к материалу или информации, необходимой для его получения с использованием информационно-телекоммуникационной сети.";

2) утратил силу с 1 октября 2014 года. – Федеральный закон от 12.03.2014 № 35-ФЗ.

Статья 5

Настоящий Федеральный закон вступает в силу с 1 августа 2013 года.

Доктрина информационной безопасности Российской Федерации

УКАЗ ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ УТВЕРЖДЕНИИ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ 05.12.2016 № 646

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее – сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

2. В настоящей Доктрине используются следующие основные понятия:

а) национальные интересы Российской Федерации в информационной сфере (далее – национальные интересы в информационной сфере) – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факто-

ров, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

е) средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

ж) система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

з) информационная инфраструктура Российской Федерации (далее – информационная инфраструктура) – совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

3. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

4. Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

5. Настоящая Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, а также других документов стратегического планирования в указанной сфере.

6. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

I. Информационная безопасность Российской Федерации

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.

2. Виды угроз информационной безопасности Российской Федерации.

3. Источники угроз информационной безопасности Российской Федерации.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

II. Методы обеспечения информационной безопасности Российской Федерации

5. Общие методы обеспечения информационной безопасности Российской Федерации.

6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни.

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.

III. Основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по ее реализации

8. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.

9. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.

IV. Организационная основа системы обеспечения информационной безопасности РФ

10. Основные функции системы обеспечения информационной безопасности Российской Федерации.

11. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.

5. Организационные основы инженерно-технической защиты информации

В организациях работа по инженерно-технической защите информации включает два этапа:

- построение или модернизация системы защиты;
- поддержание защиты информации на требуемом уровне.

Построение системы защиты информации проводится во вновь создаваемых организациях, в остальных – модернизация существующей.

Построение (модернизация) системы защиты информации и поддержания на требуемом уровне ее защиты в организации предусматривают проведение следующих основных работ:

- уточнение перечня защищаемых сведений в организации, определение источников и носителей информации, выявление и оценка угрозы ее безопасности;
- определение мер по защите информации, вызванных изменениями целей и задач защиты, перечня защищаемых сведений, угроз безопасности информации;
- контроль эффективности мер по инженерно-технической защите информации в организации.

Меры по защите информации целесообразно разделить на 2 группы: организационные и технические. В публикациях, в том числе

в некоторых руководящих документах, меры по защите делят на организационные, организационно-технические и технические. Учитывая отсутствие достаточно четкой границы между организационно-техническими и организационными, организационно-техническими и техническими мерами, целесообразно ограничиться двумя группами: организационными и техническими. При такой классификации к техническим относятся меры, реализуемые путем установки новых или модернизации используемых инженерных и технических средств защиты информации. Основу организационных мер инженерно-технической зашиты информации составляют меры, определяющие порядок использования этих средств.

Организационные меры инженерно-технической защиты информации включают, прежде всего, мероприятия по эффективному использованию технических средств регламентации и управления доступом к защищаемой информации, а также по порядку и режимам работы технических средств защиты информации. Организационные меры инженерно-технической защиты информации являются частью ее организационной защиты, основу которой составляют регламентация и управление доступом.

Регламентация – это установление временных, территориальных и режимных ограничений в деятельности сотрудников организации и работе технических средств, направленные на обеспечение безопасности информации.

Регламентация предусматривает:

- установление границ контролируемых и охраняемых зон;
- определение уровней защиты информации в зонах;

регламентация деятельности сотрудников и посетителей (разработка распорядка дня, правил поведения сотрудников в организации и вне ее и т. д.);

- определение режимов работы технических средств, в том числе сбора, обработки и хранения защищаемой информации на ПЭВМ, передачи документов, порядка складирования продукции и т. д.

Управление доступом к информации включает следующие мероприятия:

- идентификацию лиц и обращений;
- проверку полномочий лип и обращений;
- регистрацию обращений к защищаемой информации;
- реагирование на обращения к информации.

Идентификация пользователей, сотрудников, посетителей, обращений к каналам телекоммуникаций проводится с целью их надежного опознавания.

Способы идентификации рассмотрены выше.

Проверка полномочий заключается в определении прав лиц и обращений по каналам связи на доступ к защищаемой информации. Для доступа к информации уровень полномочий обращения не может быть ниже разрешенного. С целью обеспечения контроля над прохождением носителей с закрытой информацией производится регистрация (протоколирование) обращений к ним путем записи в карточках, журналах, на магнитных носителях.

Реагирование на любое обращение к информации заключается либо в разрешении доступа к информации, либо в отказе. Отказ может сопровождаться включением сигнализации, оповещением службы безопасности или правоохранительных органов, задержанием злоумышленника при его попытке несанкционированного доступа к защищаемой информации.

Технические меры предусматривают применение способов и средств. рассмотренных в данной книге.

Важнейшее и необходимое направление работ по защите информации -контроль эффективности защиты. Этот вид деятельности проводится прежде всего силами службы безопасности, а также руководителями структурных подразделений. Контроль инженерно-технической зашиты является составной частью контроля защиты информации в организации и заключается, прежде всего, в определении (измерении) показателей эффективности защиты техническими средствами и сравнении их с нормативными.

Применяют следующие виды контроля:

- предварительный;
- периодический;
- постоянный.

Предварительный контроль проводится при любых изменениях состава, структуры и алгоритма функционирования системы защиты информации, в том числе:

- после установки нового технического средства защиты или изменении организационных мер;
- после проведения профилактических и ремонтных работ средств защиты;

- предотвращение использование поддельных документов и документов лицами, которым они не принадлежат.

- после устранения выявленных нарушений в системе защиты.

Периодический контроль осуществляется с целью обеспечения систематического наблюдения за уровнем зашиты. Он проводится выборочно (применительно к отдельным темам работ, структурным подразделениям или всей организации) по планам, утвержденным руководителем организации, а также вышестоящими органами.

Наиболее часто должен проводиться периодический контроль на химических предприятиях, так как незначительные нарушения в технологическом процессе могут привести к утечке демаскирующих веществ. Для определения концентрации демаскирующих веществ регулярно берутся возле предприятия пробы воздуха, воды, почвы, снега, растительности.

Периодичность и места взятия проб определяются характером производил с учетом условий возможного распространения демаскирующих веществ, например, розы ветров и скорости воздушных потоков, видов водоемов (искусственный, озеро, болото, река и др.), характера окружающей местности и т. д. Пробы воздуха рекомендуется брать с учетом направлений ветра на высоте примерно 1,5 м в непосредственной близости от границ территории (50–100 м) и в зоне максимальной концентрации демаскирующих веществ, выбрасываемых в атмосферу через трубы. Пробы воды берутся в местах слива в водоемы к поверхностном слое и на глубине 30–50 см с последующим смешиванием. Берутся также пробы почвы и пыли на растительности. С этой целью собирают листья с нескольких деревьев и кустов на уровне 1,5–2 м от поверхности и не ранее недели после дождя.

Периодический (ежедневный, еженедельный, ежемесячный) контроль должен проводиться также сотрудниками организации в части источников информации, с которыми они работают.

Общий (в рамках всей организации) периодический контроль проводится обычно 2 раза в год. Целью его является тщательная проверка работоспособности всех элементов и системы защиты информации в целом.

Постоянный контроль осуществляется выборочно силами службы безопасности и привлекаемых сотрудников организации с целью объективной оценки уровня зашиты информации и. прежде всего, выявления слабых мест в системе защиты организации. Кроме того, такой контроль оказывает психологическое воздействие на сотрудни-

ков организации, вынуждая их более тщательно выполнять требования по обеспечению защиты информации.

Меры контроля, также как и защиты, представляют совокупность организационных и технических мероприятий, проводимых с целью проверки выполнения установленных требований и норм по защите информации. Организационные меры контроля включают:

- проверку выполнения сотрудниками требований руководящих документов по защите информации;

- проверку работоспособности средств охраны и защиты информации от наблюдения, подслушивания, перехвата и утечки информации по материально-вещественному каналу (наличие занавесок, штор, жалюзи на окнах, чехлов на разрабатываемых изделиях, состояние звукоизоляции, экранов, средств подавления опасных сигналов и зашумления, емкостей для сбора отходов с демаскирующими веществами и т. д.);

- контроль за выполнением инструкций по защите информации о разрабатываемой продукции;

- оценку эффективности применяемых способов и средств зашиты информации.

Технические меры контроля проводятся с использованием технических средств радио- и электроизмерений, физического и химического анализа и обеспечивают проверку:

- напряженности полей с информацией на границах контролируемой зоны;

- уровней опасных сигналов и помех в проводах и экранах кабелей, выходящих за пределы контролируемой зоны;

- концентрации демаскирующих веществ в отходах производства.

- степени зашумления генераторами помех структурных звуков в ограждениях;

Для измерения напряженности электрических полей используются селективные вольтметры, анализаторы спектра, панорамные приемники.

Следует также отметить, что добросовестное и постоянное выполнение сотрудниками организации требований по защите информации основываете на рациональном сочетании способов принуждения и побуждения.

Принуждение – способ, при котором сотрудники организации вынуждены соблюдать правила обращения с источниками и носите-

лями конфиденциальной информации под угрозой материальной, административной или уголовной ответственности.

Побуждение предусматривает использование для создания у сотрудников установки на осознанное выполнение требований по защите информации, формирование моральных, этических, психологических и других нравственных мотивов. Воспитание побудительных мотивов у сотрудников организации является одной из задач службы безопасности, но ее усилия найдут благодатную почву у тех сотрудников, которые доброжелательно относятся к руководству организации и рассматривают организацию как долговременное место работы. Создание условий, при которых место работы воспринимается как второй дом, является, по мнению компетентных аналитиков, одним из факторов экономического роста Японии. Поэтому эффективность защиты в значительной степени влияет климат в организации, который формируется ее руководством.

6. Методическое обеспечение инженерно-технической защиты информации

Для изучения данной темы необходимо самостоятельно рассмотреть вопросы:

6.1. Системный подход к инженерно-технической защите информации. Основные положения системного подхода к инженерно-технической защите информации.

6.1.1. Алгоритм проектирования (совершенствования) системы защиты информации. Основные этапы проектирования системы защиты информации техническими средствами.

6.2. Принципы моделирования объектов защиты и технических каналов утечки информации.

6.3. Моделирование угроз информации. Способы оценки угроз безопасности информации и расходов на техническую защиту. Моделирование каналов несанкционированного доступа к информации. Моделирование каналов утечки информации.

6.3.1. Методические рекомендации по оценке угроз радиоэлектронных каналов утечки информации. Методические рекомендации по оценке угроз вещественных каналов утечки информации. Методические рекомендации по оценке значений показателей моделирования.

6.3.2. Методические рекомендации по оценке угроз оптических каналов утечки информации. Методические рекомендации по оценке угроз акустических каналов утечки информации.

6.4. Методические рекомендации по разработке мер защитыОбщие рекомендации. Методические рекомендации по организации физической защиты источников информации. Рекомендации по повышению укрепленности инженерных конструкций. Рекомендации по повышению укрепленности ограждения периметра предприятия (организации, учреждения). Рекомендации по повышению укрепленности зданий и помещений. Выбор технических средств охраны. Выбор извещателей. Выбор шлейфов. Выбор средств наблюдения и мест их установки.

6.4.1. Рекомендации по предотвращению утечки информации. Типовые меры по защите информации от наблюдения. Типовые меры по защите информации от подслушивания. Типовые меры по защите информации от перехвата. Методические рекомендации по «чистке» помещений от закладных устройств. Меры по защите информации от утечки по вещественному каналу.

6.4.2. Рекомендации по оценке затрат на защиту и форме их представления. Комплексирование мер защиты. Оптимизация проекта системы (предложений) защиты информации.

6.4.3. Требования к оформлению проекта системы (предложений) при представлении на согласование и утверждение.

6.4.4. Тенденции развития методического обеспечения защиты информации.