Костин Н. А.

Характеристика угроз безопасности информации

Лекция 2.4

Москва, 2012

Содержание лекции:

1. **Виды угроз безопасности информации**
2. **Источники угроз безопасности информации**
3. **Опасные сигналы и их источники**

Литература:

1. ***Торокин А. А.*** **Инженерно-техническая защита информации. — М.: Гелиос АРВ, 2005.**

1.Виды угроз безопасности информации

Угрозы создают потенциальную опасность для объекта или предмета защиты.

Угрозы представляют собой состояния или действия взаимодействующих с носителями информации субъектов и объектов материального мира, которые могут привести к изменению, уничтожению, хищению и блокированию информации.

Под блокированием информации понимаются изменения условий хранения информации, которые делают ее недоступной для пользователя.

По виду реализации угрозы можно разделить на две группы:

- **физическое воздействие внешних сил на источники информации**, в результате которого возможны ее изменения, уничтожение, хищение и блокирование;
- **несанкционированное распространение носителя с защищаемой информацией от ее источника до злоумышленника**, которое приводит к хищению информации.

Угрозы, при реализации которых происходит воздействие различных сил (механических, электрических, магнитных) на источник информации, называются **угрозами воздействия на источник информации,**

а угрозы, приводящие к несанкционированному распространению носителя к злоумышленнику, — **угрозами утечки информации.**

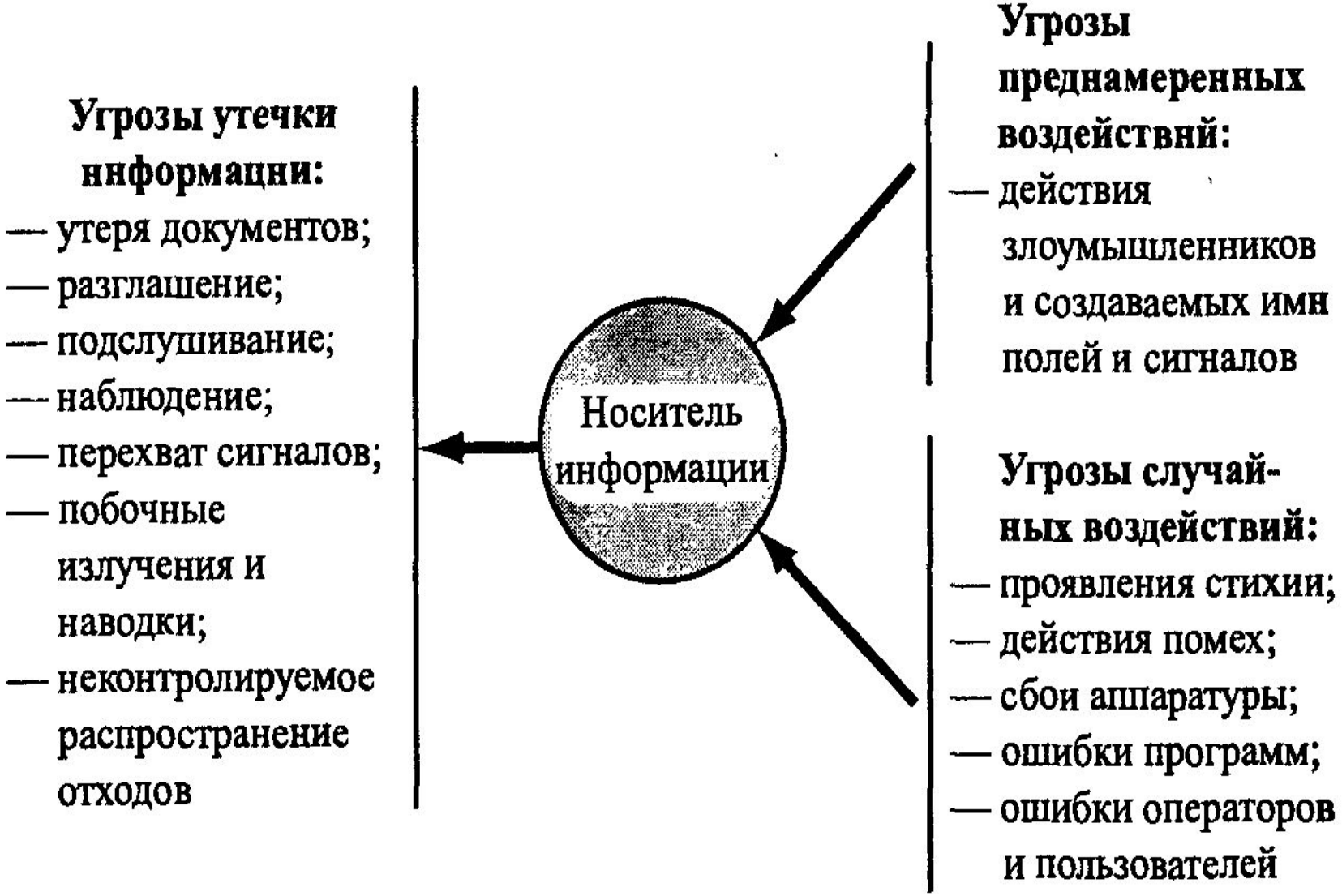

Рис. 4.1. Виды угроз

Воздействия, которые создаются злоумышленниками, являются **преднамеренными.** К ним относятся как *непосредственные воздействия людей (злоумышленников) на источник информации,* так и *воздействия полей и электрических сигналов технических средств,* создаваемых людьми с целью уничтожения, изменения или хищения информации. Например, электромагнитный импульс, возникающий во время атомного взрыва или излучения электромагнитной пушки, способен уничтожить (стереть) информацию на машинных носителях.

На источники информации постоянно действуют случайные силы, вызванные стихией природы, случайными физическими процессами в средствах хранения, обработки и передачи информации, ошибками операторов и технического персонала. Такие угрозы воздействия называются **случайными.** С целью уменьшения влияния неблагоприятных факторов окружающей среды в хранилищах архивов и музеев поддерживают определенную температуру, влажность, химический состав воздуха.

Иногда *преднамеренные* воздействия называют **несанкционированными воздействиями,**

а *случайные* — **непреднамеренными воздействиями.**

Внешние воздействия (силы), которые могут изменить, уничтожить информацию или привести к ее хищению, при распространении от источника внешней силы (внешнего воздействия) до источника информации образуют **канал несанкционированного доступа.** Если эти силы целенаправленно организуются, то канал несанкционированного доступа называется **преднамеренный,** если силы случайные, то канал несанкционированного доступа — **случайный.** Вектор движения **стихийных сил**, например природы, к источнику информации определяется физическими условиями окружающей среды и приводит к образованию **случайного канала несанкционированного доступа**.

Преднамеренный канал несанкционированного доступа организуется или создается злоумышленником. Когда он пытается проникнуть к месту хранения источника информации, то выбирает путь движения, удовлетворяющий требованиям минимизации риска быть обнаруженным и задержанным, минимизации времени движения злоумышленника. **Причин возникновения каналов несанкционированного доступа** очень много. Типовыми из них являются:

- *выполнение операции по добыванию информации органом разведки зарубежного государства, конкурента, криминальной структуры;*
- *попытки несанкционированного получения информации сотрудником организации или иным физическим лицом с целью ее продажи, шантажа, мести и другим мотивам;*
- *проявление стихийных сил (пожара, наводнения, урагана, землетрясения);*
- *неисправности программно-аппаратных средств хранения, обработки и передачи информации;*
- *ошибки в работе с программно-аппаратными средствами операторов и пользователей.*

Несанкционированное распространение носителя с информацией от ее источника к злоумышленнику называется **утечкой информации.** Она может возникнуть в результате:

- *утери источника информации (документа, продукции и др.);*
- *разглашения сведений;*
- *подслушивания;*
- *наблюдения;*
- *перехвата электромагнитных полей и электрических сигналов, содержащих защищаемую информацию;*
- *сбора отходов дело- и промышленного производства*.

Эти действия пользователя информации и злоумышленника создают угрозы утечки информации, которые в случае попадания ее к злоумышленнику приводят к утечке.

При **случайной утере** источника закрытой информации они попадут к злоумышленнику при совпадении многих условий, в том числе если источник будет найден злоумышленником или человеком, который ему его передаст. Вероятность этого невысока. Чаще найденный на территории организации источник возвращается человеку, который его потерял, или передается соответствующим должностным лицам.

Утечка информации в результате ее **непреднамеренного разглашения** происходит чаще, чем утеря источника. Даже прошедшие инструктаж люди не могут постоянно контролировать свою речь, особенно в случае повышенного эмоционального состояния. Например, в перерыве закрытого совещания его участники часто продолжают обсуждение вопросов совещания в коридоре и в местах для курения, в которых могут находиться посторонние люди. Разглашение возможно в городском транспорте, на улице, дома, на различных научных и иных конференциях. Ученые для получения признания у зарубежных коллег разглашают полученные научные сведения, содержащие государственную тайну.

Несанкционированный прием злоумышленником (его техническим средством) сигнала с защищаемой информацией и его демодуляция позволяют ему добывать эту информацию. При этом на носитель никакого воздействия не оказывается, что обеспечивает скрытность добывания. Прием оптических и иных сигналов от объектов и получение с их помощью изображений этих объектов называются **наблюдением,** прием и анализ акустических сигналов — **подслушиванием,** а прием и анализ радио- и электрических сигналов — **перехватом.**

добывания информации. Подслушивание, как и наблюдение, бывает непосредственное и с помощью технических средств. Непосредственное подслушивание использует только слуховой аппарат человека. В силу малой мощности речевых сигналов разговаривающих людей и значительного затухания акустической волны в среде распространения непосредственное подслушивание возможно на небольшом расстоянии (единицы или, в лучшем случае, при отсутствии посторонних звуков— десятки метров). Поэтому для подслушивания применяются различные технические средства. Этим способом добывается в основном семантическая (речевая) информации, а также демаскирующие признаки сигналов от работающих механизмов, машин и других источников звуков.

Наблюдение предполагает получение и анализ изображения объекта наблюдения (документа, человека, предмета, пространства и др.). При наблюдении добываются, в основном, видовые признаки объектов. Но возможно добывание семантической информации, если объект наблюдения представляет собой документ, схему, чертеж т. д. Например, текст или схема конструкции прибора на столе руководителя или специалиста могут быть подсмотрены в ходе их посещения. Также возможно наблюдение через окно помещения текста и рисунков на плакатах, развешанных на стене во время проведения совещания. Объекты могут наблюдаться непосредственно — глазами или с помощью технических средств. Различают следующие способы наблюдения с использованием технических средств:

- *визуально-оптическое;*
- *с помощью приборов наблюдения в ИК-диапазоне;*
- *наблюдение с консервацией изображения (фото- и киносъемка);*
- *телевизионное наблюдение, в том числе с записью изображения;*
- *лазерное наблюдение;*
- *радиолокационное наблюдение;*
- *радиотеплолокационное наблюдение.*

Визуально-оптическое наблюдение — наиболее древний способ наблюдения со времени изобретения линзы. Современный состав приборов визуально-оптического наблюдения разнообразен — от специальных телескопов до эндоскопов, обеспечивающих наблюдение скрытых объектов через маленькие отверстия или щели.

Так как человеческий глаз не чувствителен к ИК-лучам, то для наблюдения в ИК-диапазоне применяются специальные приборы (ночного видения, тепловизоры), преобразующие невидимое изображение в видимое.

Основной недостаток визуально-оптического наблюдения в видимом и ИК-диапазонах — невозможность сохранения изображения для последующего анализа специалистами. Для консервации (сохранения) статического изображения объекта его фотографируют, для консервации подвижных объектов производят кино- или видеосъемку.

Наблюдение объектов с одновременной передачей изображений на любое, в принципе, расстояние осуществляется с помощью средств **телевизионного наблюдения.**

Возможно так называемое лазерное наблюдение в видимом и ИК-диапазонах, в том числе с определением с высокой точностью расстояния до объекта и его координат.

Радиолокационное наблюдение позволяет получать изображение удаленного объекта в радиодиапазоне в любое время суток и в неблагоприятных климатических условиях, когда невозможны другие способы наблюдения.

При **радиотеплолокационном наблюдении** изображение объекта соответствует распределению температуры на его поверхности

Перехват предполагает несанкционированный прием радио- и электрических сигналов и извлечение из них семантической информации, демаскирующих признаков сигналов и формирование изображений объектов при перехвате телевизионных или факсимильных сигналов.

Многообразие технических средств и их комплексное применение для добывания информации порой размывают границы между рассмотренными способами. Например, при перехвате радиосигналов сотовой системы телефонной связи возможно подслушивание ведущихся между абонентами разговоров, т. е. одновременно производится и перехват и подслушивание. Учитывая неоднозначность понятий «подслушивание» и «перехват», способы добывания акустической информации целесообразно относить к подслушиванию, а несанкционированный прием радио- и электрических сигналов — к перехвату

Следовательно, угрозы утечки информации представляют собой условия и действия, при которых носитель с защищаемой информацией может попасть к злоумышленнику. Угроза утечки информации реализуется, если она попадает к злоумышленнику. Если по тем или иным причинам это не происходит, то угроза не реализуется. Например, утеря документа далеко не всегда приводит к утечке содержащейся в нем документов. Этот документ может пролежать в месте его случайного попадания сколь угодно долго или прийти в негодность под действием, например, природных факторов.

Путь несанкционированного распространения носителя информации от источника к злоумышленнику называется **каналом утечки информации.** Если распространение информации производится с помощью технических средств, то канал утечки информации называется **техническим каналом утечки информации.**

Угрозы утечки, так же как угрозы воздействия, могут быть случайными и преднамеренно создаваемыми злоумышленником. Если характеристики источников опасных сигналов злоумышленнику априори не известны, то технические каналы утечки информации являются **случайными.** Когда технический канал утечки информации организуется злоумышленником, например, с помощью закладного устройства, то такой канал утечки информации является **организованным.**

Угроза оценивается по величине ущерба, который возникает при ее реализации. Различается **потенциальный и реальный ущерб.** Потенциальный ущерб существует при появлении угрозы, реальный — при реализации угрозы. Вероятность или риск возникновения угрозы зависит от многих факторов, основными из которых являются:

- цена защищаемой информации;
- уровень защищенности информации;
- квалификация злоумышленника, его ресурс и затраты на добывание им информации;
- криминогенная обстановка в месте нахождения организации.

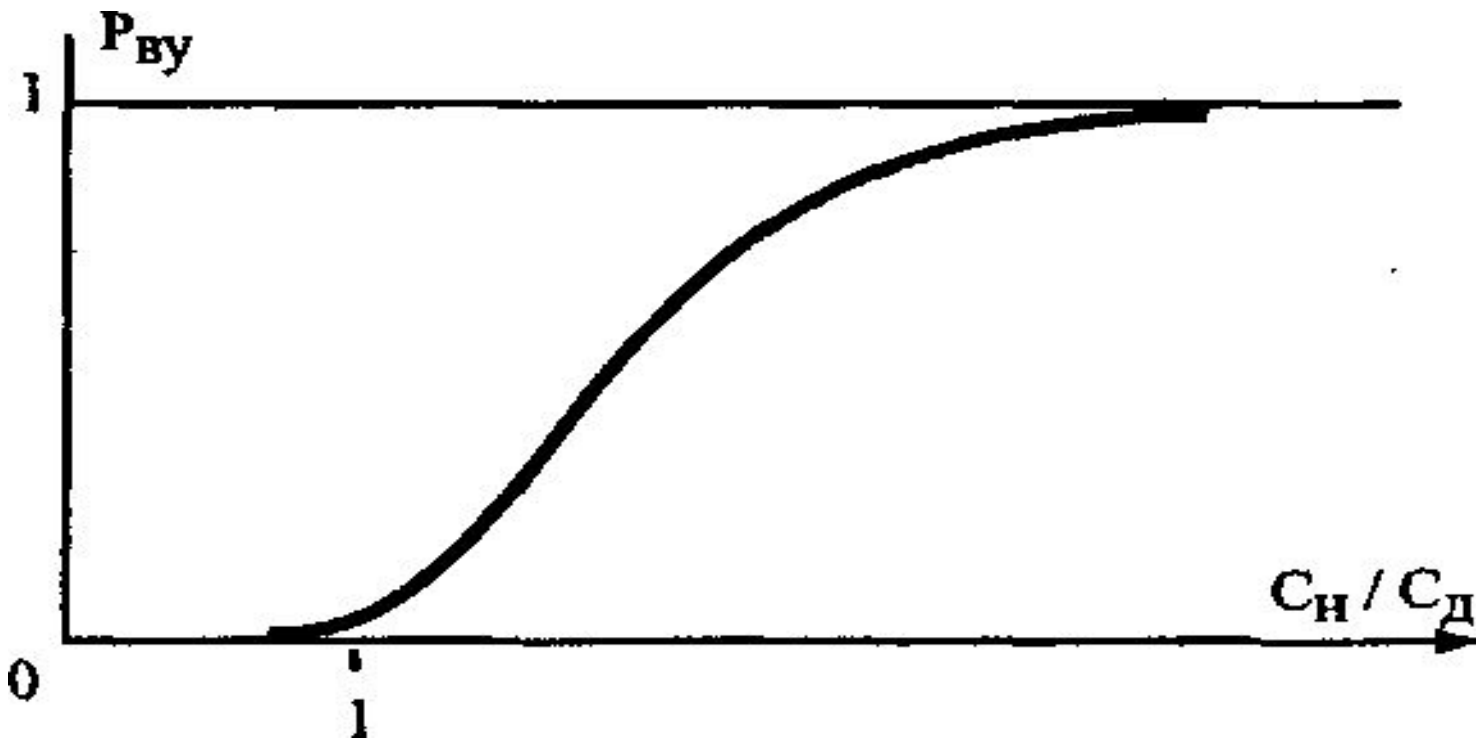

Рис. 4.2. **Зависимость вероятности возникновения угрозы воздействия от соотношения цены информации и затрат злоумышленника на ее добывание**

Уровень защищенности информации определяет затраты на добывание информации. Его рост уменьшает отношение Си / $С_д$ и, следовательно, вероятность угрозы.

Как в любой деятельности, эффективность добывания информации зависит от квалификации исполнителя. Чем выше квалификация исполнителя, тем быстрее злоумышленник доберется до источника информации и тем больше вероятность угрозы. Но квалифицированный злоумышленник тщательнее готовится к разведывательной операции и его расходы на нее выше расходов неквалифицированного злоумышленника.

Вероятность возникновения угрозы со стороны криминала зависит также от криминогенной обстановки в районе, городе, объекте федерации и в стране в целом. Там, где криминал чувствует себя хорошо, трудно ожидать, что он не заинтересуется ценной информацией.

Вероятность реализации возникшей угрозы определяется уровнем ее защиты и квалификацией злоумышленника. Чем выше уровень защиты, тем сложнее довести процесс добывания информации до конца.

2. Источники угроз безопасности информации

Применительно к информации источники угроз можно разделить на группы по видам угроз: **источники угроз воздействий на носитель информации** и **источники угроз утечки информации.** Если деятельность источников угроз направлена на несанкционированное добывание информации, то они являются источниками преднамеренных воздействий. У источников угроз случайных воздействий такая цель отсутствует. Так как целеобразование возможно только у высших животных и у человека, то источниками преднамеренных угроз являются люди, называемые **злоумышленниками.** Их деятельность по добыванию информации может быть индивидуальной или в составе различных государственных, коммерческих или криминальных структур.

В общем случае **источниками преднамеренных угроз** являются:

- *органы зарубежной разведки;*
- *органы разведки коммерческих структур государства;*
- *криминальные структуры;*
- *завербованные, психически больные или недовольные своим положением сотрудники организации.*

Наибольшие угрозы информации создают профессионалы. Любое государство создает органы разведки, обеспечивающие руководство страны информацией для принятия им политических, экономических, военных, научно-технических решений в условиях жесткой межгосударственной конкуренции. В зависимости от целей государства, его внешней политики и возможностей структуры органов разведки существенно различаются.

Самую мощную разведку имеют США. В настоящее время, согласно открытой зарубежной печати, структуру разведывательного сообщества США образуют следующие организации:

- Центральное разведывательное управление (ЦРУ);
- Министерство национальной безопасности;
- Разведывательные организации Министерства обороны США;
- Разведывательные подразделения гражданских ведомств США;
- Штаб разведки разведывательного сообщества или Центральная разведка.

ЦРУ является наиболее крупной разведывательной организацией и состоит из пяти основных директоратов (оперативного, научно-технического, информационно-аналитического, административного и планирования) и ряда самостоятельных подразделений (финансовопланового отдела, отдела шифрования, секретариата, управления по связи с общественностью и др.).

Оперативный директорат решает задачи по добыванию информации силами агентурной разведки, организации и проведения тайных операций, по осуществлению контрразведывательного обеспечения агентурной деятельности, по борьбе с терроризмом и наркобизнесом.

Научно-технический директорат проводит исследования и разработки в области технических средств разведки, эксплуатирует стационарные технические комплексы сбора, обработки и передачи информации, обеспечивает сотрудничество с научными центрами США.

Информационно-аналитический директорат проводит обработку и анализ разведывательной информации и готовит выходные документы для президента, Совета национальной безопасности, конгресса и других потребителей.

Административный директорат занимается вопросами подбора кадров на работу в ЦРУ, их подготовкой и переподготовкой, обеспечивает безопасность персонала и объектов ЦРУ и др.

Директорат планирования занимается планированием и координацией деятельности разведки.

В число разведывательных подразделений Министерства обороны входят:

-разведывательные подразделения собственно Министерства обороны;

-разведывательные подразделения Министерства армии США;

-разведывательные подразделения Министерства ВВС США;

-разведывательные подразделения ВМС США.

Основными подразделениями разведки Министерства обороны являются:

- разведывательное управление Министерства обороны (РУМО), занимающегося военно-стратегической разведкой;
- Агентство национальной безопасности (АНБ), которое ведет радиоэлектронную разведку, а также разрабатывает коды и шифры. Оно располагает одним из самых крупных центров по обработке данных, самыми мощными ЭВМ, имеет около 2 тыс. станций радиоэлектронного перехвата, численность персонала составляет более 120 тыс. человек. Силы и средства АНБ составляют основу системы радиоэлектронной разведки «Эшелон», обеспечивающей перехват информации по всему миру;
- Национальное управление военно-космической разведки.

К разведывательным организациям гражданских ведомств США относятся:

- управление разведки и исследований Госдепартамента;
- разведывательные подразделения Министерства энергетики;
- разведывательные подразделения Министерства торговли;
- разведывательные подразделения Министерства финансов;
- управление Федерального бюро расследований (ФБР).

Разведка Госдепартамента обеспечивает сбор информации, необходимой для проведения внешней политики США, участвует в разработке разведывательных операций и национальных разведывательных программ США.

Разведывательные подразделения других ведомств собирают информацию об экспортных операциях, о финансовом и валютном положении иностранных государств, об энергетике других государств, особенно об атомной энергетике, разработке и производстве ядерного оружия и по другим вопросам.

Управление контрразведки ФБР не только само ведет сбор разведывательной информации об иностранных гражданах, но и оказывает помощь другим организациям разведывательного сообщества.

В целях снижения дублирования деятельности многочисленных организаций, собирающих разведывательную информацию в интересах различных ведомств страны, координацию деятельности всех организаций разведывательного сообщества осуществляет штаб центральной разведки, который возглавляет директор ЦРУ.

Мощную разведку имеют другие развитые страны, прежде всего Россия, Великобритания, Германия, Франция, Израиль.

Состав органов разведки коммерческих структур существенно различается в зависимости от ее возможностей, прежде всего, капитала и вида деятельности. Разведка промышленных гигантов может составить конкуренцию государственной разведке. Разведкой мелкой фирмы могут заниматься всего несколько человек службы безопасности.

Организованная преступность располагает также большими финансовыми и техническими возможностями для ведения разведки и добывания информации.

Преднамеренные угрозы воздействия реализуются путем **непосредственного** и **дистанционного воздействия** на источник информации.

Для непосредственного воздействия на источник информации злоумышленник должен проникнуть к источнику информации, преодолев рубежи защиты и контролируемые зоны. Очевидно, что риск обнаружения и задержания злоумышленника силами и средствами системы защиты информации велик.

Существенно меньший риск для злоумышленника возникает при использовании им средств дистанционного воздействия на информационные параметры источника информации.

Современные **средства силового разрушающего воздействия** представляют собой по существу электромагнитное оружие, способное дистанционно вывести из строя любую информационную систему, в том числе уничтожить хранящуюся или обрабатываемую в ней информацию. Электромагнитное оружие генерирует поток кратковременных (длительностью в единицы и менее нс) и чрезвычайно мощных электрических (напряжением единицы и десятки кВ) или радиоимпульсов (мощностью в сотни и тысячи кВт), которые, распространяясь по проводам или в пространстве в виде узконаправленного луча, разрушают элементы радиоэлектронных средств обработки и хранения информации и (или) изменяют значения информационных параметров носителей информации.

Органы разведки различных структур являются источниками угроз воздействий и утечки информации. Они могут оказывать как воздействия на источник информации, так и на носители ее в виде сигналов и отходов производства.

Источники случайных угроз отличаются от преднамеренных угроз отсутствием у них целей по изменению, уничтожению, хищению и блокированию информации. **Источники угроз случайных воздействий могут быть:**

- *стихийные силы (пожар, наводнение, ураган, землетрясение и др.) и действия по их нейтрализации;*
- *пришедшие в негодное состояние инженерные конструкции, цепи электроснабжения, трубы водо- и теплоснабжения и другие элементы инфраструктуры мест установки средств информационного обеспечения;*
- *технические средства сбора, обработки, передачи и хранения информации, содержащие неисправные элементы;*
- *программы, содержащие ошибки и вирусы;*
- *неквалифицированные или плохо выполняющие свои обязанности операторы и персонал, обслуживающий программно-аппаратные средства;*
- *грызуны и насекомые в местах размещения информационных средств.*

Среди стихийных сил, которые могут в случае возникновения оказать воздействие на носитель информации, наибольшую угрозу создает пожар. Он наиболее часто происходит, может полностью уничтожить носители информации, его тушение может сопровождаться залитием мест пожара водой и пеной с не менее разрушительными для носителя информации последствиями.

В соответствии со статьей 1 Закона РФ «О пожарной безопасности» пожар — неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства». Под горением понимается сложная физико-химическая реакция окисления, сопровождающаяся выделением тепла и дыма, появлением пламени или тления. Для возникновения горения необходимо наличие «треугольника горения»: горючей среды, источника зажигания и окислителя.

Горючей средой могут быть вещества в твердом, жидком и газообразном состоянии, в том числе:

- горючие элементы несущих, ограждающих и другие конструктивные элементы части здания (обрешетка чердаков, оконные переплеты, двери);
- горючие элементы оборудования (шланги, провода и др.);
- сырье, материалы, и горючая готовая продукция;
- горючая начинка здания (мебель, материалы и др.).

Источники зажигания — это горящие или накаленные тела, электрические разряды, обладающие запасом энергии и имеющие температуру, достаточные для возникновения горения. Типичными источниками зажигания являются:

- открытое пламя от костров, спичек, технологического оборудования, паяльных ламп, газовых горелок, горящей изоляции и др.;
- тление горючих веществ (табака, торфа, хлопка в упаковке и др.);
- нагретые поверхности технологического оборудования, дымовых труб, нагревательных элементов электроплит или электрочайников, токоведущих жил кабелей при перегрузке, отопительных приборов и оборудования и др.;
- экзотермические процессы, приводящие к тепловому, микробиологическому и химическому возгоранию;
- малоразмерные сильно нагретые тела в виде раскаленных частиц, возникающих при электрогазосварочных работах и коротком замыкании цепей электропитания, тлеющие табачные изделия, искры от костров, труб, автотранспорта и др.;
- электрические искры и дуги, возникающие в электрооборудовании при выключении, в неплотных контактах электрических соединений, статического электричества, молнии.

Окислителем горения служит кислород воздуха. Его снижение в замкнутом пространстве (помещении) замедляет процесс горения, а при понижении кислорода в воздухе ниже 15% горение прекращается. Это обстоятельство положено в основу тушения пожара путем уменьшения доступа кислорода к источнику горения. Однако для эффективного тушения пожара необходимо, чтобы огнетушащее вещество не вступало в реакции с горючей средой и не способствовало развитию пожара. В зависимости от горючей среды пожары разделяются на следующие классы:

- A — твердые горючие вещества (древесина, хлопок, торф, резинотехнические изделия, пластмассы);
- B — углеводороды, спирты, эфиры, альдегиды и кетоны (нефть, бензин, жиры, смолы, ацетон и др.);
- C — горючие газы (метан, пропан, водород, ацетилен и др.);
- D — легкие и щелочные металлы и их соединения (магний, калий, натрий, алюминий и др.);
- E — радио- и электрическое оборудование под электрическим напряжением.

Обратной стороной усложнения технических средств обработки, передачи и хранения информации, постоянно внедряемых во все сферы деятельности и жизни людей, является **проблема их надежности.** Скрытые дефекты в элементах, медленно текущие химические процессы в местах контакта и другие факторы все чаще проявляются с ростом сложности радиоэлектронных средств. Хотя принимаются достаточно серьезные меры по обеспечению их надежности, выявить все скрытые дефекты невозможно.

Достаточно сослаться на опыт природы, которая для поддержания жизни живого существа постоянно обновляет его клетки и создала в его организме мощнейшую иммунную систему для борьбы с чужеродными вторжениями. Но даже эти меры, недостижимые для технических средств, далеко не всегда спасают живое существо от болезней с тяжелыми или трагическими последствиями.

Проблема усложняется еще тем обстоятельством, что вызванные неисправностями сбои в работе сложных радиоэлектронных средств не всегда оперативно выявляются, а могут проявиться в виде отложенных ошибок в работе. Например, сбои в работе процессора, вызванные чрезмерным повышением его температуры, можно заметить лишь по увеличению частоты его зависания. Учитывая, что **сбой в аппаратуре** — это **изменение электрического сигнала**, то **изменение информационного сигнала** приводит к **изменению или даже к уничтожению информации,** а изменение служебного сигнала — к блокированию информации.

Аналогичная картина наблюдается с программным обеспечением. Трудозатраты на нахождение ошибок большой программы сравнимы с трудозатратами на ее разработку. Поэтому производители программ подключают к их тестированию пользователей программ, собирая от них выявленные ими ошибки и внося исправления в очередную версию. Помимо ошибок в программе изменения и уничтожения информации вызывают вирусы, которые по мере роста их разновидностей создают серьезные угрозы безопасности информации.

Неквалифицированный или нерадивый работник представляет собой постоянную угрозу для обслуживаемой им аппаратуры и циркулирующей в ней информации. Хотя у него нет плохих намерений, но своими действиями он может причинить урон, не меньший, чем от действий врага.

Грызуны, живущие в помещениях, где находятся средства обработки информации, могут привести их в такое состояние, при котором уничтожается или видоизменяется хранящаяся в них информация. Из истории перестройки известны факты, когда крысы, объедая изоляцию проводов, превращали в металлолом корабли и самолеты. Сбои в работе аппаратуры вызывают даже тараканы, которые с удовольствием устраивают свои колонии в темных и теплых пустотах радиоэлектронной аппаратуры, изменяя своими телами параметры ее элементов и цепей.

Так как утечка информации по акустическому, оптическому и радиоэлектронному техническим каналам происходит с помощью сигналов, в информационные параметры которых записывается защищаемая информация, то **источниками угроз утечки** являются, прежде всего, **источники сигналов** в этих каналах.

Утечка информации на носителях в виде материальных тел возникает при их несанкционированном и непреднамеренном переносе к злоумышленнику. Следует отличать утечку информации на материальных телах от несанкционированного, но преднамеренного переноса таких носителей, осуществляемого злоумышленником (агентом разведки или завербованным ею сотрудником). Например, лист документа, забракованный секретаршей при печатании и выброшенный ею в корзину для бумаг, может быть перенесен уборщицей в бак для отходов, вывезен на свалку за пределы организации. На свалке он может быть обнаружен злоумышленником, следящим за отходами организации. Этот процесс распространения носителя можно рассматривать как утечку информации. Если же этот документ целенаправленно выносится из организации с целью добывания из него информации, то информация добывается агентурными методами.

3. Опасные сигналы и их источники

Носители информации в виде полей и электрического тока называются сигналами. Если информация, содержащаяся в сигналах, секретная или конфиденциальная, а сигналы могут быть приняты (перехвачены, подслушаны) злоумышленником и с них, в принципе, может быть «снята» эта информация, то такие сигналы представляют опасность для информации и называются **опасными.**

Опасные сигналы могут быть функциональными и случайными.

Функциональные сигналы создаются для выполнения радиосредством заданных функций по обработке, передаче и хранении информации. При передаче закрытой информации функциональными сигналами ее отправитель осознает потенциальные угрозы безопасности содержащейся в сигналах информации. Принимает он необходимые меры или нет, это его выбор. По небрежности или злому умыслу, он иногда пренебрегает этими мерами. Например, на раннем этапе становления рыночных отношений бизнесмены часто по радиотелефонной сотовой связи разглашали сведения, составляющие коммерческую тайну. Более опытные люди при разговоре по открытой телефонной линии для скрытия от посторонних ушей некоторых аспектов разговора применяют так называемый «эзоповский» язык, т. е. слова со скрытым смыслом, не всегда понятным посторонним лицам.

К основным источникам функциональных сигналов относятся:

- передатчики (источники сигналов) систем связи;
- передатчики радиотехнических систем;
- излучатели акустических сигналов гидролокаторов и акустической связи;
- люди как источники условных сигналов.

Средства систем связи образуют наиболее многочисленную и разнообразную группу источников сигналов с семантической информацией. К системам и средствам связи относятся системы и средства радиосвязи, проводной, радиорелейной, космической и оптической связи, ионосферной, тропосферной и метеорной радиосвязи. Они занимают ведущее место в обеспечении информационного обмена во всех сферах общественно-производственной деятельности и личной жизни людей.

Источниками радиосигналов, излучаемых в окружающее пространство, являются стационарные и мобильные радиопередающие устройства систем радиосвязи, а электрических сигналов, передаваемых по проводам, — телефонные, телеграфные, факсимильные аппараты, ПЭВМ, объединенные в сети, модемы аппаратуры передачи данных, телевизионные камеры кабельного телевидения и др.

В последнее время для передачи информации в качестве **источников сигналов применяются также лазеры оптических средств связи.** Уступая радиосигналам по дальности распространения, в особенности при неблагоприятных климатических условиях, оптические системы связи имеют значительно лучшие параметры по полосе пропускания и помехоустойчивости. Кабели волоконно-оптических линий связи с широкими возможностями по уменьшению величины затухания света и снижения себестоимости изготовления постепенно вытеснят металлические кабели проводных систем электросвязи.

Радио-, электрические и световые сигналы циркулируют как внутри организации, так и распространяются на большие, а при их ретрансляции — на любые расстояния. По телефону можно переговорить с абонентом в любом месте Земли, радиосигналы соответствующей частоты и мощности способны донести информацию также до любой ее точки.

Учитывая широкое применение средств связи и большие дальности распространения сигналов, **перехват сигналов средств связи представляет один из эффективных и широко распространенных методов добывания информации.** Сигналы средств связи содержат не только семантическую информацию, но и информацию о признаках сигналов и местоположении их источников. Такая информация характеризует технические решения новых средств и их возможности, что представляет интерес как для внутреннего, так и для внешнего (зарубежного) конкурента.

К **радиотехническим системам и средствам** относятся средства радиолокации, радионавигации, радиотелеметрии, радиотелеуправления, а также радиопротиводействия (радиоэлектронной борьбы).

Среди радиотехнических систем и средств значительную долю занимают радиолокационные станции, предназначенные для наблюдения воздушного пространства и земной поверхности в радиодиапазоне. Возможности радиолокаторов по добыванию информации определяются в основном характеристиками радиотехнических сигналов и распределением их энергии в пространстве (диаграммой направленности). К радиотехническим системам и средствам, характеристики сигналов которых интересуют органы добывания разведки, относятся также **системы и средства радиопротиводействия (радиоэлектронной борьбы),** предназначенные для нарушения систем управления войсками и оружием противника в военное время.

Так как **радио- и гидролокационные станции** создают техническую основу для противоракетной, противовоздушной и противолодочной обороны, то параметры сигналов новейших локаторов вызывают большой интерес у разведки других государств. Очевидно, что сигнальные признаки разрабатываемых радио- и акустических средств интересуют также конкурентов в России и других государствах, создающих подобную технику.

Радионавигационные средства и системы предназначены для определения местоположения объектов на суше, воде, в воздухе и в космосе. **Радиотелеметрические средства и системы** обеспечивают измерение и передачу различных физических величин удаленных объектов, а средства и системы радиотелеуправления — управление ими.

Но потенциальная опасность для информации, содержащейся в функциональных сигналах, априори известна ее владельцу. Он при распространении сигналов или идет на осознанный риск, или может принять меры по его снижения до допустимого значения. **Риск уничтожения, изменения или хищения информации — это та цена, которую объективно платит владелец информации для ее передачи современными способами.** Он может передать информацию не с помощью сигналов, а с почтой или курьером, что часто делается, если цена информации очень высока, например при доставке дипломатических документов. Но при этом резко возрастают финансовые затраты и снижается оперативность. Поэтому электронные формы хранения и передачи информации вытесняют традиционные — на материальных телах.

Однако работа радиоэлектронных средств, используемых для приема, обработки, хранения и передачи сигналов, а также различных электрических приборов сопровождается явлениями и физическими процессами, которые могут создавать побочные радио- и электрические сигналы. Если эти сигналы по тем или иным причинам могут содержать секретную или конфиденциальную информацию и к ним возможен доступ технических средств злоумышленника, то опасность для этой информации существенно выше, чем для аналогичной информации, но содержащейся в функциональных сигналах. Такие случайно возникающие сигналы называются **случайными опасными сигналами.** Эти сигналы возникают в силу объективных физических процессов, часто независимо от пользователя технического средства. Без проведения специальных исследований его пользователь может и не знать о наличии случайных сигналов и тех угроз, которым подвергается секретная или конфиденциальная информация. В этом состоит существенное отличие функциональных опасных сигналов от случайных опасных сигналов.

К техническим средствам обработки, передачи и хранения, создающим опасные сигналы, относятся:

- средства телефонной проводной связи;
- средства мобильной телефонной и радиосвязи;
- средства электронной почты;
- средства электронной вычислительной техники;
- аудиоаппаратура и средства звукоусиления;
- радиоприемные устройства;
- видеоаппаратура;
- телевизионные средства;
- средства линейной радиотрансляции и оповещения.

Кроме того, **случайные опасные сигналы создают электрические приборы,** в том числе:

- средства системы электрочасофикации;
- средства охранной сигнализации;
- средства пожарной сигнализации;
- средства размножения документов;
- средства системы кондиционирования и вентиляции воздуха;
- бытовые приборы, оргтехника и иное производственное оборудование, имеющее в своем составе элементы преобразования акустической информации в электрические сигналы (акустоэлектрические преобразователи);
- электропроводящие коммуникации здания, проходящие через контролируемую зону.

Характеристики опасных случайных сигналов радиоэлектронных средств и электрических приборов априори неизвестны ни злоумышленнику, ни их пользователю. Для их обнаружения и определения характеристик проводят специальные проверки и исследования этих средств и приборов.

В зависимости от принадлежности циркулирующей (обрабатываемой, хранящейся, передаваемой) в технических средствах и системах информации к секретной (конфиденциальной) или несекретной эти средства и системы делятся на **основные технические средства и системы (ОТСС)** и **вспомогательные технические средства и системы (ВТСС).**

К **основным техническим средствам и системам** относятся средства (системы) и их коммуникации (линии связи), обеспечивающие обработку, хранение и передачу защищаемой информации. Из этого не следует, что ОТСС должны обрабатывать только защищаемую информацию. В условиях рынка это экономически нецелесообразно. В общем случае ОТСС могут использоваться для решения задач, не связанных с сохранением тайны, но в них априори приняты меры по защите информации.

Если в технических средствах (системах) приема, обработки, хранения и передачи информации такие меры отсутствуют, то они относятся к вспомогательным. **Вспомогательные технические средства и системы (ВТСС) не предназначены для обработки защищаемой информации,** но могут размещаться совместно с ОТСС в контролируемой зоне. Последнее замечание имеет принципиальное значение, так как именно близость размещения ВТСС к ОТСС вынуждает рассматривать вспомогательные средства и системы как потенциальные источники опасных сигналов.

К **ВТСС отнесены**:

- различного рода телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
- средства и системы кондиционирования;

средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания и радиоприемники.);

- средства электронной оргтехники;
- средства и системы электрочасофикации;
- иные технические средства и системы.

Вопросы для самопроверки

1. Сущность угрозы безопасности информации.
2. Виды угроз безопасности информации и их отличия.
3. Основные угрозы воздействия на источники информации и ее утечки.
4. Основные источники угроз информации, содержащей государственную тайну.
5. Факторы, влияющие на риск угрозы безопасности информации.
6. Чем отличаются опасные случайные сигналы от функциональных опасных сигналов?
7. Основные источники опасных случайных сигналов.
8. Классы пожаров.

Чем отличаются основные технические средства и системы от вспомогательных технических средств и систем?