Каналы утечки информации

Вводная часть

В ходе данного занятия будет рассмотрено понятие «каналы утечки информации», их классификация и основные физические процессы каналов утечки информации.

(**Слайд № 2**). **Актуальность** данного занятия определяется тем, что утечка информации является серьезной проблемой как для государственных учреждений, так и для коммерческих организаций. Новые технологии перехвата важных данных появляются и совершенствуются постоянно. Не всегда за ними успевают меры защиты, связано это с тем, что до внедрения новая технология должна пройти стадии апробации, оценки, внедрения. Тем не менее предвидение возможных угроз и использование всего комплекса ресурсов, предлагаемого современной наукой и техникой, помогут обеспечить надежную защиту.

Отрасль, связанная с разработкой средств и методов хищения коммерческой тайны, развивается очень быстро. Сегодня на рынке присутствуют в основном зарубежные компании, специализирующиеся на разработке и реализации шпионских устройств; зарубежные и отечественные программисты и хакеры, совершенствующие шпионский софт; многочисленные посредники, адаптирующие для рынка технологии спецслужб; продавцы оборудования, среди которого:

- радиопередатчики;
- замаскированные и закладные устройства;
- мобильные телефоны с активированными полицейскими функциями (передачи звуковой конфиденциальной информации, формируемой в зоне вокруг аппарата);
- аппаратно-промышленные комплексы ведения корпоративной разведки.

Поэтому на современном этапе эффективность защиты информации определяется тем, что необходимым условием реализации интегрального подхода к системе защиты информации является исследование возможных каналов утечки и их характеристик и блокирование всех технических каналов утечки и несанкционированного доступа к информации.

Таким образом, выше изложенный материал определяет необходимость изучения каналов утечки информации (рис. 1).

Рисунок 1 – Каналы утечки информации

В ходе занятия будут рассмотрены следующие учебные вопросы:

1. Каналы утечки информации. Виды и классификация каналов утечки информации.

2. Физические процессы каналов утечки информации.

Первый учебный вопрос: «Каналы утечки информации. Виды и классификация каналов утечки информации»

При создании или передаче информации в каком-либо виде возникает угроза нарушения ее конфиденциальности, или угроза утечки информации. В зависимости от вида представления информации, способы получения доступа к ней различаются и принято выделять различные каналы утечки информации, т.е. пути, которыми может быть получен доступ к конфиденциальной информации.

В **ГОСТ Р 53114-2008** «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» определены термины в области утечки информации.

Утечка информации – неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками.

К каналам утечки информации относится разглашение информации и получение информативного сигнала злоумышленником посредством ее перехвата.

Разглашение информации – несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации.

Информативный сигнал – сигнал, по параметрам которого может быть определена защищаемая информация.

Данный информативный сигнал перехватывается техническими средствами, применяемыми злоумышленниками.

Перехват информации – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Т.е. под перехватом понимают получение разведывательной информации путем приема электромагнитного и акустического излучения пассивными средствами приема, расположенными, как правило, на безопасном расстоянии от источника информации.

Существует два метода перехвата: непосредственный перехват и электромагнитный перехват.

Непосредственный перехват – это перехват, осуществляемый либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Электромагнитный перехват – это перехват, осуществляемый за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д., т.е. перехват с технических средств, имеющих побочные электромагнитные излучения и наводки. Данный перехват может

осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Таким образом, **канал утечки информации** – совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах контролируемой зоны, охватывающей автоматизированную информационную систему, или вне ее. Т.е. это физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Необходимо отметить, что каналы утечки информации характеризуются как скрытые каналы.

В соответствии с **ГОСТ Р 53113.1-2008** «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов».

Скрытый канал – это канал, непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

Например, манипулирование битами в пакетах протоколов связи может использоваться как скрытый метод передачи сигналов. Природа скрытых каналов такова, что предотвратить существование всех возможных скрытых каналов затруднительно или даже невозможно. Однако такие каналы часто используются «троянскими» программами. Следовательно, принятие мер по защите от «троянских» программ снижает риск использования скрытых каналов. Предотвращение неавторизованного доступа к сети, а также политики и процедуры, препятствующие неправильному использованию информационных услуг персоналом, способствуют защите от скрытых каналов.

Для создания канала утечки информации или скрытого канала применяется агент нарушителя.

Агент нарушителя – это лицо, программное, программно-аппаратное или аппаратное средство, действующие в интересах нарушителя.

Рассмотрим ***типовой механизм функционирования скрытого канала***.

Скрытые каналы используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на автоматизированную информационную систему, которая не обнаруживается средствами контроля и защиты.

Опасность скрытых каналов основана на предположении постоянного доступа нарушителя безопасности к информационным ресурсам организации и воздействии через эти каналы на информационную систему для нанесения максимального ущерба организации.

Общая схема механизма функционирования скрытых каналов в автоматизированной информационной системе представлена на рис. 2.

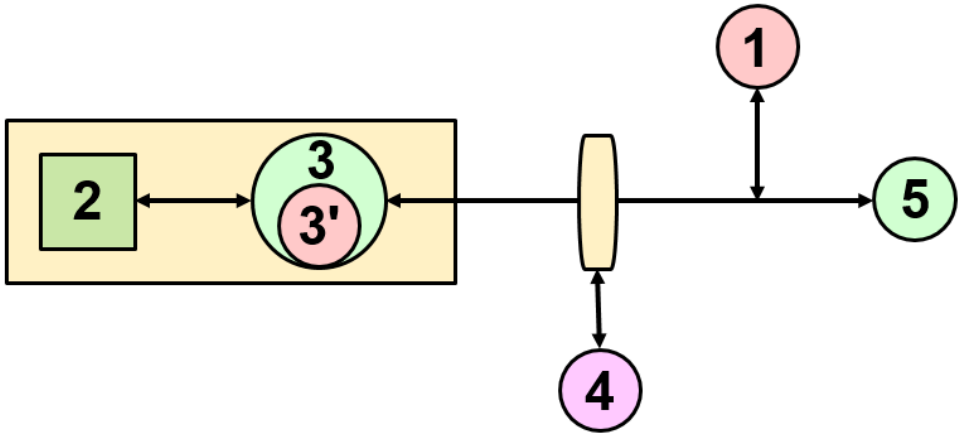

Рисунок 2 – Схема механизма функционирования скрытых каналов в автоматизированной информационной системе

где:

1 – нарушитель безопасности (злоумышленник), целью которою валяется НСД (информации ограниченною доступа либо несанкционированное влияние на АИС;

2 – информация ограниченного доступа либо критически важная функция;

3 – субъект, имеющий санкционированный доступ к 2;

3' – агент нарушителя безопасности, находящийся в замкнутом контуре с 2 и взаимодействующий с 2 от имени субъекта 3;

4 – инспектор (программное, программно-аппаратное, аппаратное средство или лицо), контролирующий(ее) информационное взаимодействие 3. пересекающее замкнутый контур, отделяющий объект информатизации от внешней среды;

5 – субъект, находящийся вне замкнутого контура, с которым 3 осуществляет санкционированное информационное взаимодействие.

Взаимодействие между субъектами 3 и 5 является санкционированным и необходимым для правильной работы АИС. Задача агента *3* заключается в

том, чтобы обеспечить регулярное интерактивное взаимодействие между агентом и злоумышленником. Агент должен передать информацию ограниченного доступа 2 злоумышленнику *1* либо по команде злоумышленника *1* оказать воздействие на критически важную функцию 2. Скрытность канала взаимодействия между злоумышленником *1* и агентом *3'* заключается в том, что субъект *3*, инспектор *4* и субъект 5 не обнаруживают факт передачи информации или команды.

Скрытые каналы позволяют злоумышленнику регулярно интерактивно осуществлять взаимодействие со своим агентом, внедренным в автоматизированную информационную систему.

При выявлении каналов утечки информации необходимо рассматривать всю совокупность элементов системы, включающую основное оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, электробытовые приборы и др.

К **факторам, способствующим утечки информации** относятся:

• недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) 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.

Следует помнить о **внутренних каналах утечки информации**, связанных с действиями администрации и обслуживающего персонала, с качеством организации режима работы, тем более что обычно им не придают должного внимания. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, съем информации с ленты принтера и плохо стертых дискет, использование производственных и технологических отходов, визуальный съем информации с дисплея и принтера, несанкционированное копирование и т. п.

К **внешним каналам утечки информации** относятся:

- телекоммуникационные сети, линии связи и коммунальные сети, выходящие за пределы контролируемой зоны;

- электромагнитные, визуально-оптические, материально-вещественные, информационные, выходящие за пределы контролируемой зоны.

Все **каналы проникновения в систему и утечки информации** разделяют на прямые и косвенные.

Под ***косвенными*** понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы.

В качестве косвенных каналов утечки информации большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения с установленными в них основными и вспомогательными техническими средствами, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

Прямые каналы могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов. Для использования прямых каналов необходимо проникновение в помещения, где расположены компоненты системы.

Кроме этого, по **типу основного средства**, используемого для реализации угрозы все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

По способу получения информации потенциальные каналы утечки информации можно разделить на:

• акустические (включая и акустопреобразовательные). Связаны с распространением звуковых волн в воздухе или упругих колебаний в других средах;

• электромагнитные (в том числе магнитные и электрические);

• визуально-оптические (наблюдение, фотографирование). В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т. п.;

• материально-вещественные (бумага, фото, магнитные носители, отходы и т. п.);

• информационные. Связаны с доступом к элементам телекоммуникационных систем, носителям информации, самой вводимой и выводимой информации, к программному обеспечению, а также с подключением к линиям связи.

Иной возможности для переноса информации в природе не существует.

В соответствии с **ГОСТ Р 53113.2-2009** «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов» **классификация скрытых каналов по механизму передачи информации** подразделяют на:

- скрытые каналы по памяти;
- скрытые канал по времени;
- скрытые статистические каналы;
- скрытые каналы по пропускной способности.

Скрытые каналы по памяти основаны на наличии памяти, в которую передающий субъект записывает информацию, а принимающий - считывает ее. Скрытость каналов по памяти определяется тем, что сторонний наблюдатель не знает того места в памяти, где записана скрываемая информация. Скрытые каналы по памяти предполагают использование ресурсов памяти, однако способ использования памяти не учитывается разработчиками системы защиты и поэтому не может выявляться используемыми средствами защиты.

Скрытые каналы по памяти, в свою очередь, подразделяют на:

- скрытые каналы, основанные на сокрытии информации в структурированных данных;
- скрытые каналы, основанные на сокрытии информации в неструктурированных данных.

Скрытые каналы, основанные на сокрытии информации в структурированных данных, используют встраивание данных в информационные объекты с формально описанной структурой и формальными правилами обработки. Например, внутренний формат файлов, используемых современными текстовыми процессами, содержит ряд полей, не отображаемых при редактировании файла, поэтому они могут быть использованы для вставки скрытой информации.

Скрытые каналы, основанные на сокрытии информации в неструктурированных данных, используют встраивание данных в информационные объекты без учета формально описанной структуры (например, запись скрытой информации в наименее значимые биты изображения, не приводящая к видимым искажениям изображения).

Скрытые каналы по времени предполагают, что передающий информацию субъект модулирует с помощью передаваемой информации некоторый изменяющийся во времени процесс, а субъект, принимающий информацию, в состоянии демодулировать передаваемый сигнал, наблюдая несущий информацию процесс во времени. Например, в многозадачной операционной системе центральный процессор является разделяемым информационно вычислительным ресурсом для прикладных программ. Модулируя время занятости процессора, приложения могут передавать друг другу нелегальные данные.

Скрытый статистический канал использует для передачи информации изменение параметров распределений вероятностей любых характеристик системы, которые могут рассматриваться как случайные и описываться вероятностно-статистическими моделями. Скрытость таких каналов основана на том, что получатель информации имеет меньшую неопределенность в определении параметров распределений наблюдаемых характеристик системы, чем наблюдатель, не имеющий знаний о структуре скрытого канала. Например, появление реальной, но маловероятной комбинации в присланном пакете в заданный промежуток времени может означать сигнал к сбою в компьютерной системе.

Скрытые каналы по пропускной способности подразделяют на:

- канал с низкой пропускной способностью;
- канал с высокой пропускной способностью.

Скрытый канал является каналом с низкой пропускной способностью, если его пропускной способности достаточно для передачи ценных информационных объектов минимального объема (например, криптографические ключи, пароли) или команд за промежуток времени, на протяжении которого данная передача является актуальной.

Скрытый канал является каналом с высокой пропускной способностью, если его пропускная способность позволяет передавать информационные объекты среднего и большого размера (например, текстовые файлы, изображения, базы данных) за промежуток времени, на протяжении которого данные информационные объекты являются ценными. Для решения сложных задач может использоваться комбинация скрытых каналов, опирающихся на различные механизмы передачи.

Таким образом, существуют следующие виды **каналов утечки информации** относят:

- ✓ акустическое излучение информативного речевого сигнала;
- ✓ электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы контролируемой зоны (территория, здание, часть здания, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств);
- ✓ виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- ✓ несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;
- ✓ воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
- ✓ хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- ✓ побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;
- ✓ наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны;

- ✓ радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- ✓ радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации «закладок», модулированные информативным сигналом;
- ✓ радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- ✓ прослушивание ведущихся телефонных и радиопереговоров;
- ✓ просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств.

На этом изложение первого учебного вопроса завершено.

Второй учебный вопрос: «Физические процессы каналов утечки информации»

Для принятия правильного решения по защите информации необходимо понимание физических процессов, создающих возможность утечки информации по рассмотренным в предыдущем вопросе каналам утечки информации.

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве излучения, которые в той или иной степени связаны с обрабатываемой информацией и являются объектом для перехвата.

Правомерно предполагать, что образованию каналов утечки информации способствуют также определенные обстоятельства и причины технического характера (несовершенство схемных решений, эксплуатационный износ элементов изделия).

В любых технических средствах существуют те или иные физические преобразователи, которые выполняют соответствующие им функции, основанные на определенном физическом принципе действия. Однако помимо основных своих функций такие преобразователи в соответствии со своей физической природой способны порождать и дополнительные каналы утечки. Знание всех типов физических преобразователей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих каналы утечки информации.

Входе изучения второго учебного вопроса мы рассмотрим физические процессы для типовых каналов утечки информации, это:

1. Акустические каналы утечки информации;
2. Вибрационные, каналы утечки информации;

3. Преобразователи информации:
   - преобразователи аудиоинформации;
   - индуктивные преобразователи. Микрофонный эффект;
   - пьезоэлектрический преобразователь;
   - оптические преобразователи;
4. Электромагнитные каналы утечки;
5. Визуально-оптические каналы утечки;
6. Информационные каналы утечки информации.

В соответствии с представленными типами каналов утечки информации, мы начнем с **акустических каналов утечки информации**.

Наиболее ценной акустической информацией чаще всего является речь. Частоты речевых сигналов 16 – 20 000 Гц.

Один и тот же звук разные люди произносят по-разному (своего рода речевой почерк). Звуки речи не одинаково информативны: гласные содержат мало информации о смысле речи, а глухие согласные наиболее информативны.

Мерой силы звукового ощущения является громкость звука. Минимальная громкость соответствует порогу слышимости, максимальная – порогу болевого ощущения. Оба порога зависят от частоты звука. Человеческому уху свойственно изменение порога слышимости: в условиях тишины слышен писк комара, а в условиях шума трудно услышать громкую речь.

Качество речи оценивается ее разборчивостью, представляющей собой статистическую характеристику речи, принимаемой на фоне шумов. ***Разборчивость*** – это отношение числа правильно понятых элементов речи (звуков, слогов, слов) к общему числу переданных по каналу элементов. Она может характеризовать качество канала только в среднем значении, допуская флуктуации в ту или иную сторону. Разборчивость речи определяется экспериментально с помощью так называемых артикуляционных испытаний. Объективные измерительные и расчетные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант. Формантами называются максимумы текущего спектра речи, которые заполняют весь речевой диапазон. Доказано, что восприятие человеком формант обладает свойством аддитивности, т. е. каждый участок речевого диапазона вносит свой вклад в общую разборчивость речи. В акустических измерениях используются октавные или третьоктавные частотные полосы. Для октавного анализа вклады частот русской речи равны следующим значениям:

Частотная полоса, кГц – 0,25; 0,5; 1; 2; 4; 8.

Разборчивость формант, % – 6,7; 12,5; 21,2; 29,4; 25; 5,2.

От качественного приема (без искажений и помех) каждой частотной полосы зависит суммарная разборчивость. Предельное значение разборчивости формант, при которой возможно понимание смысла речевого сообщения, равно 15 %, что соответствует 25 %-й разборчивости слогов. Задача оценки канала утечки сводится к измерению или вычислению разборчивости речи и сравнению полученного значения с предельным.

Важным является то, какое качество принятого сигнала может обеспечить используемый канал. Для оценки *акустического канала* при работе с речевой информацией также применяется такая характеристика, как разборчивость речи. Она зависит от следующих факторов:

• ослабления речи в канале;

• реверберации звука (это процесс постепенного уменьшения интенсивности звука при его многократных отражениях);

• уровня вибрационных и акустических шумов в местах установки датчиков;

• чувствительности самих датчиков.

Оперативная оценка этих факторов осложняется тем, что вибрационные и акустические сигналы не поддаются точному расчету. Качество каналов съема оценивают экспериментальным путем с помощью акустических измерений, имитирующих ситуацию контроля информации, кроме компьютерной информации.

Шумы и помехи, возникающие в месте установки датчика, вызываются многочисленными естественными источниками: автомобильным транспортом, работой механических машин, технических средств в помещениях, разговорами в смежных помещениях и т. п. Характерная особенность шумов – их не стационарность, т. е. изменение уровня во времени. Эти изменения зависят от времени суток (вечером уровни шумов намного меньше, чем днем), от дня недели (в выходные дни уровни шумов снижаются), от погодных условий. Наибольшие шумы – уличные, которые создаются автомобильным транспортом, листвой (при наличии ветра), а также дворовые. В здании источниками шумов являются люди (разговоры, шаги), работа механизмов, водопровода, лифта. Средние значения акустических шумов на улице составляют 60...75 дБ и зависят от интенсивности движения автомашин в районе расположения объекта. Разница в уровне шумов от максимального до минимального может составлять до 30 дБ. Следует иметь в виду, что существующая норма допустимого уровня акустических шумов в рабочих помещениях равна 50 дБ. Этот уровень можно брать в качестве расчетного, если неизвестны конкретные показатели шумности в смежных посторонних помещениях. Все приведенные значения шумов даны для широкополосных источников помех, которые не различаются человеческим ухом, но маскируют акустическую информацию для шпионской аппаратуры.

Поэтому помехи предназначены для скрытия (маскировки) полезного акустического сигнала, распространяющегося в виде акустических колебаний. Маскирующие свойства помех проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона.

Таким образом, ***акустические колебания*** в помещении складываются из шумов источников, находящихся внутри помещения, и шумов источников вне помещения.

Основные пути прохождения акустических волн из помещения:

• воздушный перенос: прохождение через открытые окна, двери, щели, поры, вентиляционные воздуховоды;

• материальный перенос: прохождение через материал стены или по трубам отопления, газопровода, водопровода в виде продольных колебаний;

• мембранный перенос: передача колебаний посредством поперечных колебаний перегородки (стекла, стены и пр.).

При рассмотрении первого пути говорят об акустическом канале утечки, второй и третий образуют вибрационный канал.

В воздушных каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными мини передатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т. п. В этом случае прием осуществляется, как правило, на специальные приемные устройства. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с телефонного аппарата.

Поэтому, создавая защиту от акустических каналов утечки информации, необходимо определить фактический уровень разговорной речи (аудио записи), уровень естественных шумов и рассчитать требуемый уровень маскирующих шумов и помех.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции.

Следующий тип каналов утечки информации – **вибрационные, или структурные, каналы утечки информации**. В данных каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких как стекла окон, зеркал, картин и т. п., создается оптико-электронный, или лазерный, канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие обычно в ближнем инфракрасном диапазоне волн и известные

как «лазерные микрофоны». Дальность перехвата составляет несколько сотен метров (рис. 3).

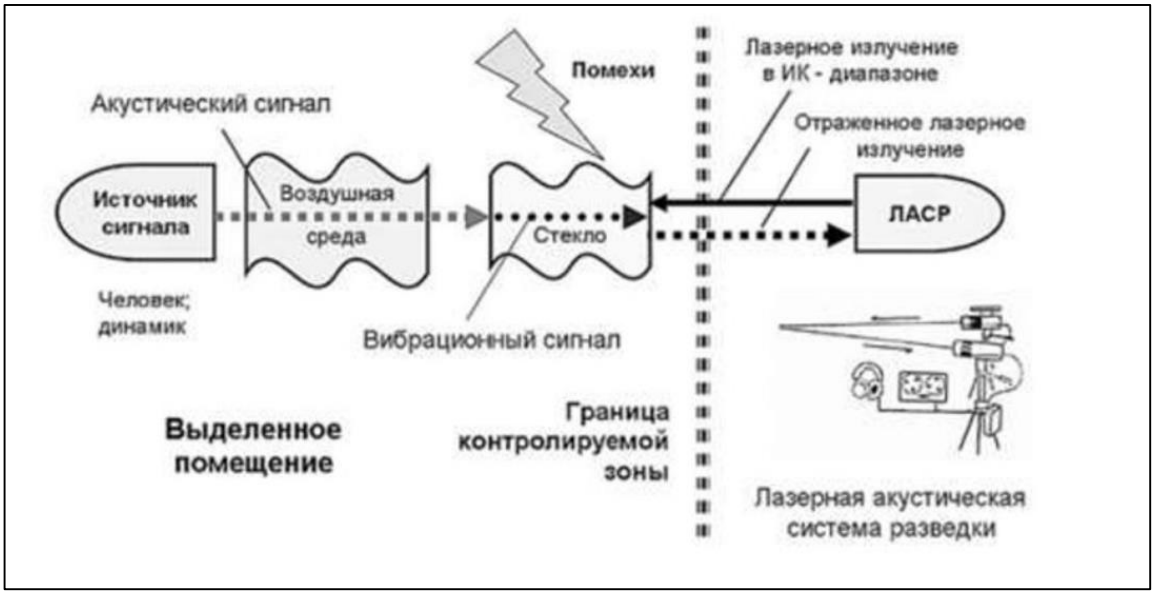

Рисунок 3 – Схема канала перехвата речевой информации с использованием лазерной акустической системы разведки

Следующий тип каналов утечки информации – **преобразователи информации.**

Преобразователи аудиоинформации. Преобразователем является прибор, который преобразует изменения одной физической величины в изменения другой.

Акустическая энергия, возникающая при разговоре, может вызвать акустические (т. е. механические) колебания элементов электронной аппаратуры, что в свою очередь приводит к появлению или изменению электромагнитного излучения.

Любой преобразователь характеризуется определенными параметрами. Наиболее важными из них являются:

• чувствительность – отношение изменения выходного сигнала к изменению сигнала на его входе;

• разрешающая способность – наибольшая точность, с которой осуществляется преобразование;

• линейность – равномерность изменения выходного сигнала в зависимости от входного;

• инертность (время отклика) – время установления выходного сигнала в ответ на изменение входного сигнала;

• рабочая полоса частот – частотный диапазон, в пределах которого воздействие на входе преобразователя создает на выходе допустимый уровень сигнала.

По физической природе имеется значительное количество различных первичных преобразователей информации, среди которых выделяются следующие группы:

• индуктивные;
• емкостные;
• пьезоэлектрические;
• оптические преобразователи.

Наиболее чувствительными к акустическим воздействиям элементами радиоэлектронной аппаратуры являются катушки индуктивности и конденсаторы переменной емкости.

Индуктивные преобразователи. Микрофонный эффект. Рассмотрим акустическое воздействие на катушку индуктивности с сердечником. Механизм и условия возникновения ЭДС (электродвижущая сила) индукции в такой катушке сводятся к следующему. Под воздействием акустического давления появляется вибрация корпуса и обмотки катушки. Вибрация вызывает колебания проводов обмотки в магнитном поле, что и приводит к появлению 70 ЭДС индукции на концах катушки. Она зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки. Данный эффект непосредственно используется в электродинамических микрофонах, поэтому получил название микрофонного эффекта.

Индуктивные преобразователи информации (рис. 4) подразделяются на:

- электромагнитные;
- электродинамические;
- магнитострикционные.

Рисунок 4 – Индуктивные преобразователи информации

К *электромагнитным преобразователям* относятся такие устройства как громкоговорители, электрические звонки (в том числе и вызывные звонки телефонных аппаратов), электрорадиоизмерительные приборы.

Типичный образец индуктивного акустоэлектрического преобразователя – электромеханический вызывной звонок телефонного аппарата, микрофонный эффект которого проявляется при положенной телефонной трубке. По тому же принципу образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения. Акустические колебания воздействуют на якорь реле. Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

Динамические головки прямого излучения, устанавливаемые в абонентских громкоговорителях, имеют достаточно высокую чувствительность к акустическому воздействию и довольно равномерную в речевом диапазоне частот амплитудно-частотную характеристику, что обеспечивает высокую разборчивость речевых сигналов.

В магнитоэлектрическом измерительном приборе имеются подвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита. Рамка соединена со стрелкой, конец которой перемещается по шкале измерения. Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции (рис. 5).

Рисунок 5 – Схема индуктивных датчиков

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор. Различие между магнитоэлектрическим и электромагнитным приборами сводится к тому, что в электромагнитном приборе вместо постоянного магнита используется электромагнит.

Следует отметить, что ЭДС микрофонного эффекта возникает и может использоваться в состоянии покоя прибора, когда он не применяется для конкретных измерений.

Примерами индукционных акустоэлектрических преобразователей являются различные трансформаторы (повышающие, понижающие, входные, выходные, питания и др.).

Трансформатор состоит из двух (или более) изолированных друг от друга катушек (обмоток) с разными числами витков и замкнутого сердечника из мягкой стали или феррита (рис. 6).

Рисунок 6 – Трансформатор

Акустическое влияние на сердечник и обмотку трансформатора (например, на входной трансформатор усилителя звуковых частот) приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается в разы, соответствующие коэффициенту трансформации.

Трансформаторы обладают важным свойством – магнитострикцией.

Магнитострикция – изменение размеров и формы кристаллического тела при намагничивании – вызывается изменением энергетического состояния кристаллической решетки в магнитном поле и, как следствие, расстояний между узлами решетки. Наибольших значений магнитострикция достигает в ферро- и ферритомагнетиках, в которых магнитное взаимодействие частиц особенно велико.

Обратное по отношению к магнитострикции явление – Виллари-эффект, т. е. изменение намагничиваемости тела при его деформации.

Виллари-эффект обусловлен изменением под действием механических напряжений доменной структуры ферромагнетика, определяющей его намагниченность. В усилителях с очень большим коэффициентом усиления входной трансформатор на ферритах способен преобразовывать механические колебания в электрические.

Емкостные преобразователи. Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения.

Емкость конденсатора зависит от расстояния между пластинами. Воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости (рис. 7).

Рисунок 7 – Емкостные преобразователи информации

Конденсаторы переменной емкости с воздушным диэлектриком являются одним из основных элементов перестраиваемых колебательных контуров генераторных систем. Они устроены так, что система пластин вдвигается в другую систему пластин, образуя конденсатор переменной емкости. Изменяющееся акустическое давление, воздействуя на такой конденсатор, изменяет его емкость, а, следовательно, и характеристики устройства, в котором он установлен.

Пьезоэлектрический преобразователь. Изучение свойств твердых диэлектриков показало, что некоторые из них поляризуются не только с помощью электрического поля, но и в процессе деформации при механических воздействиях на них. Поляризация диэлектрика при механическом воздействии называется прямым пьезоэлектрическим эффектом. Этот эффект имеется у кристаллов кварца и у всех сегнетоэлектриков. У пьезокристаллов наблюдается и обратное явление. Если пластину, вырезанную из пьезокристалла, поместить в электрическое поле, зарядив металлические обкладки, то она поляризуется и деформируется, например, сжимается. При перемене направления внешнего электрического поля сжатие пластинки сменяется ее растяжением (расширением). Такое явление называется обратным пьезоэлектрическим эффектом (рис. 8).

Рисунок 8 – Пьезоэлектрические преобразователи информации

Кварцевые пластины широко используются в пьезоэлектрических микрофонах, охранных датчиках, стабилизаторах, генераторах электрического микрофона.

Оптические преобразователи. К оптическим преобразователям относятся приборы, преобразующие световую энергию в электрическую и обратно (рис. 9).

Рисунок 9 – Оптические преобразователи информации

Что касается технических каналов утечки информации, то в оптических системах опасным является акустооптический эффект. **Акустооптический эффект** – это явление преломления, отражения или рассеяния света, вызванное упругими деформациями стеклянных отражающих поверхностей или волоконно-оптических кабелей под воздействием звуковых колебаний. Волоконные световоды как преобразователи механического давления в изменение интенсивности света являются источником утечки акустической информации за счет акустооптического (или акустоэлектрического) преобразования – микрофонного эффекта в волоконно-оптических системах передачи информации (используется также в охранных системах).

Основным элементом оптического кабеля волоконно-оптических систем является волоконный световод в виде тонкого стеклянного волокна цилиндрической формы. Волоконный световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с различными оптическими характеристиками (показателями преломления). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки –

создание лучших условий отражения на границе сердцевина-оболочка и защита от излучения в окружающее пространство (рис.10).

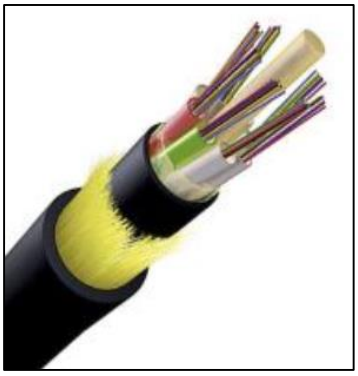

Рисунок 10 – Оптический кабель

Передача волны по световоду осуществляется за счет отражений ее от границы сердечника и оболочки, имеющих разные показатели преломления. В современных волоконно-оптических системах в процессе передачи информации используется модуляция источника света по амплитуде, интенсивности и поляризации.

Внешнее акустическое воздействие на волоконно-оптический кабель приводит к изменению его геометрических размеров (толщины), что вызывает изменение пути движения света, т. е. приводит к изменению интенсивности, причем пропорционально значению этого давления.

При слабом закреплении волокон в разъемном соединителе световодов проявляется акустический эффект модуляции света акустическими полями. Акустические волны вызывают смещение соединяемых концов световода относительно друг друга. Таким образом осуществляется амплитудная модуляция излучения, проходящего по волокну, что способствует утечки информации.

Следующий тип канала утечки информации – **электромагнитные каналы утечки**.

Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Вокруг проводника, по которому протекает ток I, вызванный напряжением U, создается магнитное поле с напряженностью H и электрическое поле с напряженностью E.

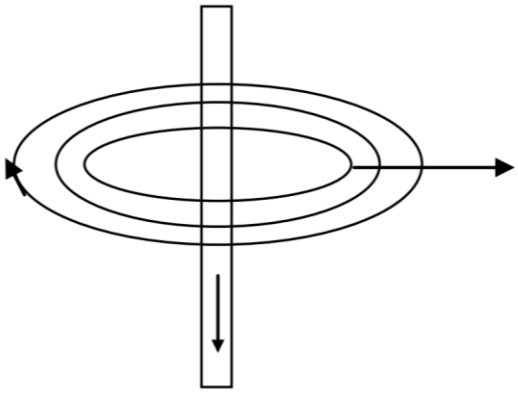

Рисунок 2 – Распределение магнитного и электрического поля вокруг проводника с током

Изменение во времени тока приводит к изменению во времени электрического и магнитного полей. Вызванные изменением тока в проводнике изменяющиеся во времени электрическое и магнитное поля представляют собой единое изменяющееся электромагнитное поле, распространяющееся в пространстве, свойства которого целиком и полностью описываются уравнениями Максвелла.

Известно, что характер поля изменяется в зависимости от расстояния до передающего устройства. Поле делится на две зоны: ближнюю и дальнюю.

В дальней зоне (начиная от расстояний, больших 6λ от источника возмущения) электрическое поле принимает плоскую конфигурацию и распространяется в виде плоской волны, энергия которой делится поровну между электрической и магнитной компонентами. Дальняя зона – это область пространства, в которой распространение от источника существенно превышает длину волны. Граница между дальней и ближней зонами находится на расстоянии около 0,5 м от источника излучения для частоты 100 МГц и 50 м для частоты 1 МГц.

В ближней зоне преобладает магнитная либо электрическая составляющая поля. Сильные магнитные поля, как правило, создаются цепями с низким волновым сопротивлением, большим током и малым перепадом напряжений.

Для поля с преобладающей электрической компонентой волновое сопротивление существенно больше, а для преобладающего магнитного поля – существенно меньше значения волнового сопротивления для плоской волны (Z = 377 Ом).

Изменение тока во времени может носить импульсный характер или подчиняться любому другому закону. Каждый такой процесс на основе известного из математики преобразования Фурье может быть представлен в виде суммы гармонических колебаний с различными амплитудами для каждой частоты, причем частоты изменяются в пределах от нуля до бесконечности. Зависимость амплитуд этих гармонических составляющих от частоты – это спектр сигнала (в рассматриваемом случае –

электромагнитного излучения). Спектр характеризует распределение энергии в поле излучения. В зависимости от того, на каких частотах устройство излучает наиболее интенсивно, излучатели электромагнитных сигналов подразделяют на низкочастотные, высокочастотные и оптические.

Низкочастотными излучателями электромагнитных колебаний в основном являются звукоусилительные устройства различного функционального назначения и конструктивного исполнения. В ближней зоне этих устройств наиболее мощным выступает магнитное поле информативного сигнала. Такое поле усилительных систем достаточно просто обнаруживается и принимается посредством магнитной антенны и селективного усилителя звуковых частот.

К *группе высокочастотных излучателей относятся* ВЧ-автогенераторы, модуляторы ВЧ-колебаний и устройства, генерирующие паразитные высокочастотные колебания по различным причинам и в различных условиях.

Источниками сигнала выступают ВЧ-генераторы радиоприемников, телевизоров, измерительных генераторов, мониторы компьютеров, модуляторы ВЧ колебаний. Довольно опасным источником высокочастотных колебаний могут быть усилители и другие активные элементы технических средств в режиме паразитной генерации за счет нежелательной положительной обратной связи.

В качестве высокочастотного излучателя рассматривается любое устройство, содержащее элементы с нелинейными характеристиками (диоды, транзисторы, микросхемы), порождающими нежелательные составляющие высокочастотного характера.

Спектр излучения обычно не поддается аналитическому расчету, т. к. его форма зависит от многих факторов; прежде всего это следующие:

• рабочие частоты устройства, их гармоники и комбинационные частоты;

• расположение и длина проводников;

• расположение и конструкция реактивных элементов (конденсаторов и индуктивных катушек);

• тип корпуса, наличие в нем щелей, отверстий и т. п.

При анализе спектра следует разделять информативное ПЭМИ и неинформативное ПЭМИ, а также реальные возможности восстановления информации из принятого ПЭМИ.

Наиболее опасными являются следующие виды излучений и наводок:

• электромагнитные излучения элементов ТСОИ (носителем информации является электрический ток, напряжение, частота или фаза которого изменяются по закону информационного сигнала);

• электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС (в результате внешних воздействий информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную

модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство);

• электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСПИ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом);

• наводки электромагнитных излучений ТСОИ (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС);

• просачивание информационных сигналов в цепи электропитания (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала);

• просачивание информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.);

• съем информации с использованием закладных устройств, представляющих собой минипередатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны.

Особое внимание следует обратить на перехват информации при ее передаче по каналам связи. Это вызвано тем, что в данном случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам, особенно в случае использования радиоканала. В зависимости от вида канала связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств.

Электромагнитный канал перехвата информации широко применяется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям.

Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком. Поэтому чаще

используется индукционный канал перехвата, не требующий контактного подключения к каналам связи.

Следующий тип каналов утечки информации – **визуально-оптические каналы утечки**.

В последнее время стало уделяться большое внимание утечке визуальной информации, получаемой в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т. п.

Для документирования результатов наблюдения проводится съемка объектов с помощью фотографических и телевизионных средств, соответствующих условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

Следующий тип каналов утечки информации – **информационные каналы утечки информации**.

Информационный канал может быть разделен на следующие каналы:

• канал коммутируемых линий связи;
• канал выделенных линий связи;
• канал локальной сети;
• канал машинных носителей информации;
• канал терминальных и периферийных устройств.

Утечка информации из канала связи при использовании специальных технических средств съема информации была рассмотрена выше.

В последнее время наиболее динамично развиваются методы съема компьютерной информации. В этом направлении используются:

• аппаратные закладки;
• вредоносные программы.

Основные возможности несанкционированного доступа связаны с использованием специального математического обеспечения, включающего в себя такие составляющие, как компьютерные вирусы, «логические бомбы», «троянские кони», программные закладки и т. п.

Вредоносная программа – программа, предназначенная для несанкционированного копирования, модификации, блокирования, уничтожения компьютерной информации.

Часто вредоносная программа доставляется к месту постоянного размещения через привлекательную для пользователя программу («троянскую» программу). То есть для «троянской» программы характерно наличие встроенной структуры или функции, скрытно выполняющей вредоносные действия. При запуске или на этапе инсталяции параллельно идут два процесса: документированный и недокументированный.

Вредоносные программы можно разделить на две большие категории:

1) вирусы. Основные свойства вирусов: паразитическое существование, размещение внутри программного файла или в другом месте, способность к саморазмножению – копированию, выраженные деструктивные функции. Основная угроза со стороны вирусов – угроза целостности;

2) программные закладки. Основные свойства: скрытность работы на всех этапах жизненного цикла, явно выраженные «шпионские» функции, частое отсутствие механизма саморазмножения, хотя возможно наличие механизма самоликвидации.

В настоящее время известно большое количество программных закладок, основные функции которых следующие:

• слежение за пользователем;
• раскрытие паролей, ключей;
• изучение обрабатываемой информации.

Вредоносные программы могут быть внедрены в прикладные программы, утилиты и сервисные программы, подсистему безопасности, реестр, ядро, командный интерпретатор, BIOS, драйверы устройств, аппаратные средства. ВП, внедренные на уровень ядра и ниже, невидимы для пользователя.

На этом изложение второго учебного вопроса завершено.

Литература

1. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».

2. ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов».

3. ГОСТР 53113.2-2009 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов».

Заключение

Из представленного учебного материала вам необходимо уяснить термины в области «угрозы информации» и «утечки информации» и классификации данных категорий.

Доцент кафедры БИТ Д.Власкин