**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ**

**«ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ П. О. СУХОГО»**

Заочный факультет

Кафедра «Информационные технологии»

**РЕФЕРАТ**

по дисциплине: «Основы защиты информации»

на тему: **«**Защита информации от утечки по техническим каналам**»**

Выполнил: студент гр. ЗИТ-51 Никитенко А.И.

Проверил: доцент

Кравченко О.А.

Гомель 2022

**ОГЛАВЛЕНИЕ**

Введение…………….…………………………………………………………......3

1. Классификация технических каналов утечки информации…………….........4
2. Акустические каналы утечки информации……………………………...........6
3. Канал побочного электромагнитного излучения……………………………11

Заключение……………………………………………………………………….13

Список использованных источников…………………………………………...14

**ВВЕДЕНИЕ**

Информационные технологии коренным образом меняют облик материального производства, позволяют экономить материальные ресурсы, создавать новые приборы и системы, в общем, в буквальном смысле изменяют наши представления о времени и пространстве.

Однако широкое внедрение в жизнь информационных технологий, управляющих жизненно важными процессами, к сожалению, сделало их достаточно уязвимыми со стороны естественных воздействий среды и искусственных воздействий со стороны человека. Возникла проблема обеспечения безопасности информационных систем в широком смысле слова или защиты информации в более узкой постановке.

Защита информации необходима для предотвращения утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы.

Способов передачи конфиденциальной информации на расстоянии существует множество. Однако создать абсолютно надежный, недоступный для других канал связи не всегда представляется возможным, из-за чего возникают утечки информации.

1. **КЛАССИФИКАЦИЯ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ**

Утечки информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной.

Естественные каналы утечки информации возникают при обработке информации техническими средствами(электромагнитные каналы утечки информации) за счет побочных электромагнитных излучений, а также вследствие наводок информационных сигналов в линиях электропитания технического средства обработки информации, соединительных линиях вспомогательных технических средств и систем (ВТСС) и посторонних проводниках (электрические каналы утечки информации). К специально создаваемым каналам утечки информации относятся каналы, создаваемые путем внедрения в техническое средство обработки информации электронных устройств перехвата информации (закладных устройств) и путем высокочастотного облучения технического средства обработки информации.

Среди распространенных причин утечки информации выделяют такие версии:

* недостаточная охрана чужих данных (организацией или доверенным лицом).
* неправильное обращение с устройствами, которые хранят информацию (по техническим причинам).

Технический канал утечки информации (ТКУИ) – совокупность источника конфиденциальной информации, среды распространения и средства технической разведки для перехвата информации (рис 1.1).

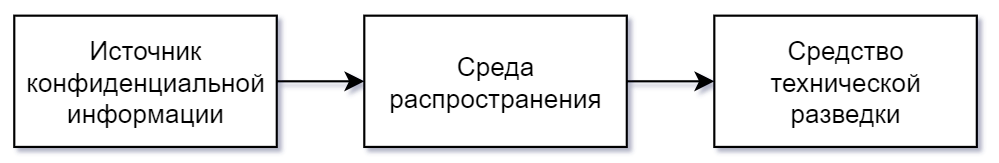


Рис. 1.1 – Технический канал утечки информации

Источники конфиденциальной информации:

* человек;
* электронная аппаратура;
* документы (содержание);
* здания и сооружения (внешний вид).

Среда распространения конфиденциальной информации:

* воздушная;
* твердые вещества (строительные конструкции);
* электрические цепи.

Средства технической разведки:

* визуально-оптические (оптические увеличительные приборы);
* оптоэлектронные (приборы ночного видения, тепловизоры и т.д.);
* акустические (закладные устройства, направленные микрофоны, электронные стетоскопы и т.д.);
* фотографические;
* электронные (для перехвата сигналов в проводных коммуникациях).

По физическим принципам возникновения каналы утечки информации можно разделить на следующие группы (рис. 1.2):

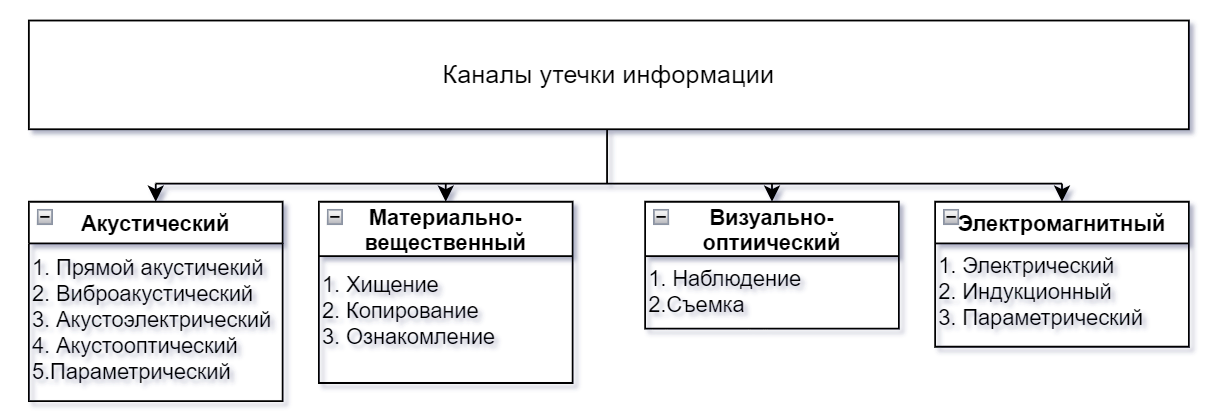


Рис. 1.2 Классификация каналов утечки информации

1. **АКУСТИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ**

Голосовой аппарат человека является первичным источником акустических колебаний, которые представляют собой возмущения воздушной среды в виде волн сжатия и растяжения (продольных волн). Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний.

Различного рода преобразователи акустических и вибрационным колебаний являются вторичными источникам. К последним относятся громкоговорители, телефоны, микрофоны и другие устройства.

Акустические каналы утечки информации разделяют на акустические (прямые), вибрационные, акустоэлектрические, акустооптические и параметрические.

В **акустических(прямых) каналах** утечки информации средой распространения речевых сигналов является воздух, и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны. Микрофоны соединяются с портативными звукозаписывающими устройствами или специальными миниатюрными передатчиками. Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информации. Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому каналу, соединительным линиям, посторонним проводникам, инженерным коммуникациям в ультразвуковом диапазоне частот, телефонной линии с вызовом от внешнего телефонного абонента (рис 2.1).

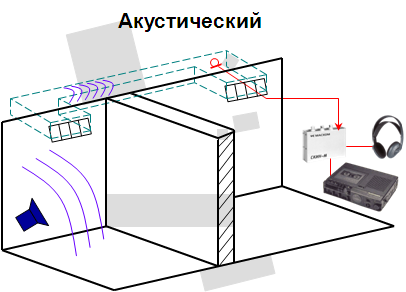


Рис. 2.1 – Акустический(прямой) канал утечки информации

В **виброакустических каналах** утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.). Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры) (рис. 2.2).

Вибродатчик, соединенный с электронным усилителем называют электронным стетоскопом. Электронный стетоскоп позволяет осуществлять прослушивание речи с помощью головных телефонов и ее запись на диктофон.

По виброакустическому каналу также возможен перехват информации с использованием «стетоскопных» ЗУ. В них для передачи информации используется радиоканал, поэтому   такие   устройства   часто   называют радиостетоскопами. Реально, также возможно использование ЗУ с передачей информации по оптическому каналу инфракрасном диапазоне волн, а также по ультразвуковому каналу (по инженерным коммуникациям).

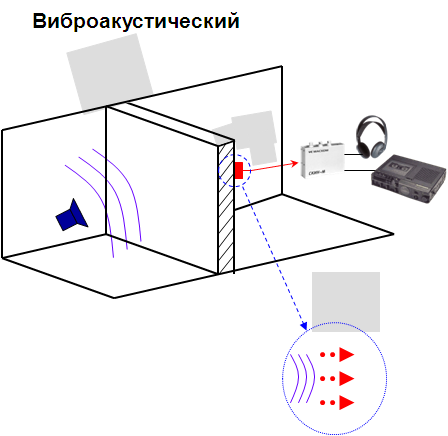


Рис. 2.2 – Виброакустический канал утечки информации

**Акустоэлектрические  каналы**  утечки  информации  возникают за  счет преобразований акустических сигналов в электрические (рис. 2.3).

Некоторые трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов и т.п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающих по этим элементам, в соответствии с изменениями воздействующего акустического поля.

Вспомогательные технические средства и системы (ВТСС), кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи (АЭП). К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Эффект АЭП называют «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват акустоэлектрических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Наиболее часто такой канал используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы КЗ.



Рис. 2.3 – Акустоэлектрический канал утечки информации

**Акустооптический (оптико-электронный или лазерный)** канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих под действием акустического речевого сигнала отражающих поверхностей помещений (оконных стекол, зеркал и т.д.). Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация (рис. 2.4).

Для организации такого канала предпочтительным является использование зеркального отражения лазерного луча. Однако, при небольших расстояниях до отражающих поверхностей (порядка нескольких десятков метров) может быть использовано диффузное отражение лазерного излучения.

Для перехвата речевой информации по данному каналу используются сложные лазерные системы, которые в литературе часто называют «лазерными микрофонами». Работают они, как правило, в ближнем инфракрасном диапазоне длин волн.



Рис. 2.4 – Акустооптический канал утечки информации

**Параметрические каналы** утечки информации. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС (рис. 2.5). При этом изменяется взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в помещениях, где ведутся конфиденциальные разговоры.

Параметрический канал утечки информации может быть реализован и путем ВЧ облучения помещения, где установлены ЗУ, имеющие элементы, параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются под действием акустического (речевого) сигнала.

При облучении помещения мощным ВЧ сигналом, в таком ЗУ при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. А специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала.

Для реализации такого канала необходимы специальный передатчик с направленным излучением и приемник.

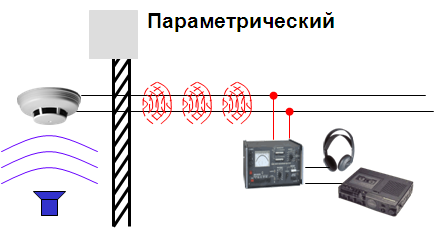


Рис. 2.5 – Параметрический канал утечки информации

1. **КАНАЛ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ**

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные электромагнитные излучения (ПЭМИ), которые в той или иной степени связаны с обрабатываемой информацией (электромагнитный канал).

Физические явления, лежащие в основе появления этих излучений, имеют различный характер, но тем не менее они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторой «побочной системе связи», образованной источником излучения, средой и средством перехвата информации.

Регистрация средством технической разведки ПЭМИ источника информации (персональный компьютер и др.) распространяющихся через воздушную среду обуславливает возникновение индукционного канала утечки информации (рис. 3.1).

Кроме того, в индукционном канале используется эффект возникновения вокруг себя кабеля ПЭМИ при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками. Индукционные датчики применяются в основном для перехвата информации с симметричных высокочастотных кабелей.

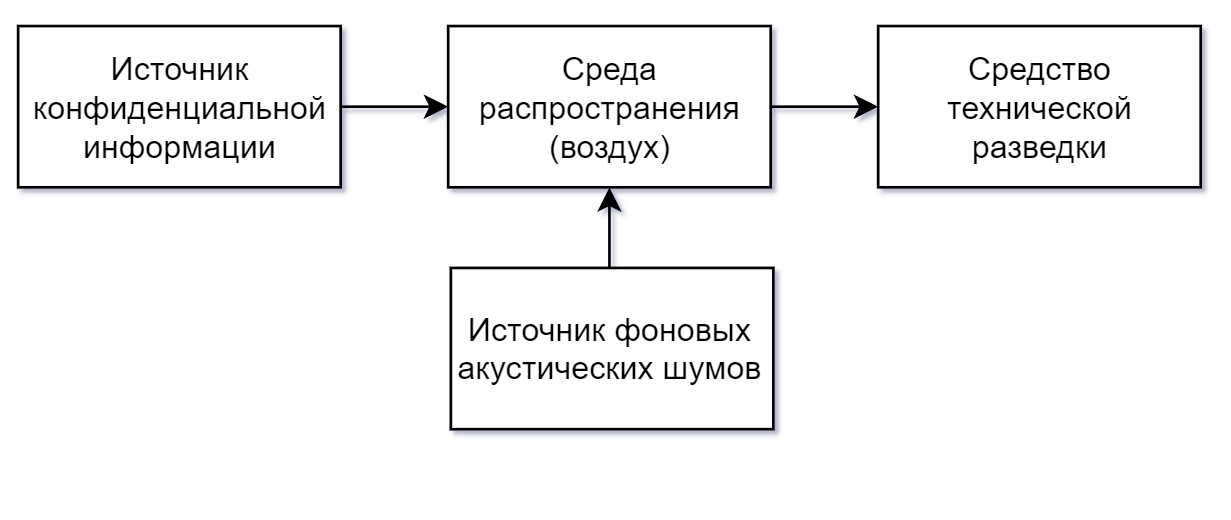


Рис. 3.1 – Структурная схема индукционного канала утечки информации

Электрический канал утечки информации (рис. 3.2) возникает за счет наводок ПЭМИ технических средств обработки информации (ТСОИ) на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны (сеть электропитания, цепи охранной и пожарной сигнализации и т.д.). В этом случае наводка обусловлена тем, что данные проводники выступают в качестве случайных антенн (цепь ВТСС или посторонние проводники, способные принимать ПЭМИ).

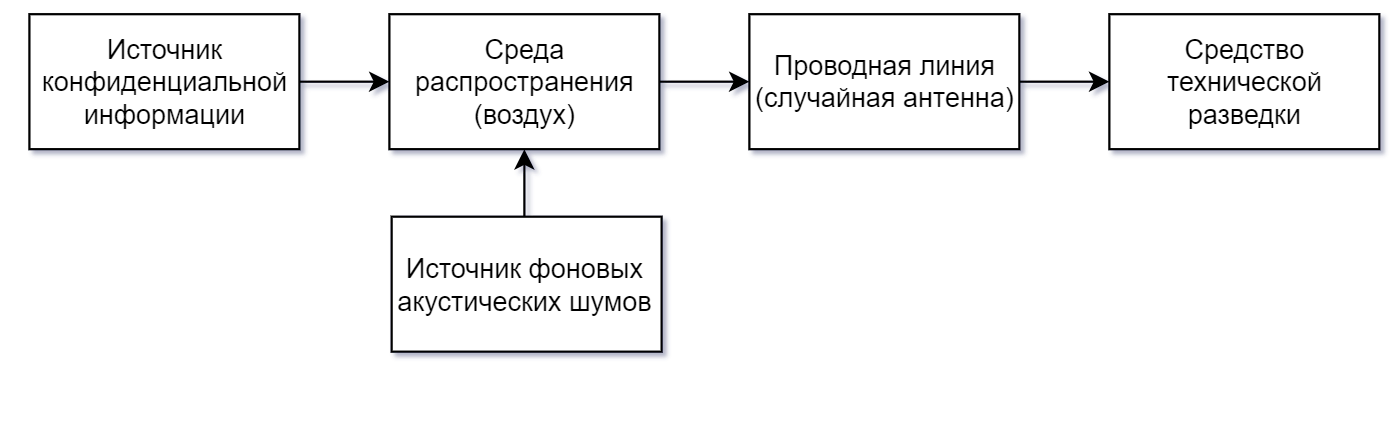


Рис. 3.2 – Структурная схема электрического канала утечки информации

Наводки электромагнитных излучений ТСОИ возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или лини ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСОИ и посторонних проводников.

Параметрический электромагнитный канал может возникать в процессе облучения ТСОИ побочными электромагнитными излучениями ВТСС, вследствие чего может возникнуть переизлучение электромагнитной волны, которое будет содержать информацию, обрабатываемую в ТСОИ.

**ЗАКЛЮЧЕНИЕ**

В наше время никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность данных в компьютерных сетях.

В вычислительной технике понятие безопасности является весьма широким. Оно подразумевает и надежность работы компьютера, и сохранность ценных данных, и защиту информации от внесения в нее изменений неуполномоченными лицами, и сохранение тайны переписки в электронной связи. Разумеется, во всех цивилизованных странах на безопасности граждан стоят законы, но в вычислительной технике правоприменительная практика пока не развита, а законотворческий процесс не успевает за развитием технологий, и надежность работы компьютерных систем во многом опирается на меры самозащиты.

Подводя итоги, можно утверждать, что угроза информационному ресурсу возрастает с каждым днем, подвергая в панику ответственных лиц в банках, на предприятиях и в компаниях во всем мире.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Лыньков Л.М. Основы защиты информации и управления интеллектуальной собственностью: учеб.-метод. Пособие / Л.М. Лыньков, В.Ф. Голиков, Т.В. Борботько. –Минск: БГУИР, 2013. – 243с.
2. Мурашко, И. А. Защита компьютерной информации: пособие по одноим. дисциплине для студентов специальности 1-40 01 02 «Информационные системы и технологии (по направлениям)» днев. и заоч. форм обучения / И. А. Мурашко. – Гомель : ГГТУ им. П. О. Сухого, 2015. – 48 с
3. Урбанович, П. П. У69 Защита информации методами криптографии, стеганографии и обфускации : учеб.-метод. пособие для студентов специальности 1-98 01 03 «Программное обеспечение информационной безопасности мобильных систем», направления специальности 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)», специальности 1-40 01 01 «Программное обеспечение информационных технологий» специализации 1-40 01 01 10 «Программирование Интернет-приложений» / П. П. Урбанович. – Минск : БГТУ, 2016. – 220 с.