Программно-аппаратные средства зашиты информации

Тема 1. Основные понятия и методы защиты объектов информатизации

1. Основные понятия информационной безопасности.
2. Компоненты информационной безопасности.
3. Классификация угроз безопасности информатизации.
4. Место программно-аппаратных средств защиты в системе комплексной защите объектов информатизации.
5. Технические каналы утечки информации

Литература

1. Кемпф В.А. Технические средства защиты информации. Учебное пособие. –Барнаул: Барнаульский юридический институт МВД России, 2010.–32 с.
2. Сидорин Ю.С. Технические средства защиты информации: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. 141 с.
3. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А. П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
4. Скрипник Д.А. Общие вопросы технической защиты информации. Режим доступа http://www.intuit.ru/goto/course/techproi/

Основные понятия

Терминология в области безопасности и защиты информации изложена в:
- международных стандартах в области информационной безопасности;
- федеральных законах России;
- указах Президента и постановлениях Правительства России;
- государственных и отраслевых стандартах;
- специальных нормативных (руководящих) документах ФСТЭК России и ФСБ

ИНФОРМАЦИЯ И ФОРМЫ ЕЁ ПРОЯВЛЕНИЯ

Информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

ФОРМЫ ИНФОРМАЦИИ

сведения - запечатлённые в организме результаты отражения движения объектов материального мира

сообщения– *набор знаков*, с помощью которых сведения могут быть *переданы* другому организму и *восприняты* им

«данные» - *факты, понятия или команды, представленные в формализованном виде* (можно рассматривать как разновидность сообщений, предназначенных для автоматизированной обработки с использованием средств вычислительной техники)

Основные понятия

Злоумышленник – это субъект, который незаконным путем пытается добыть, изменить или уничтожить информацию законных пользователей.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - злоумышленником.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации

Основные понятия

Целью защиты информации является обеспечение информационной безопасности.

Безопасность информации - состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, доступность и целостность.

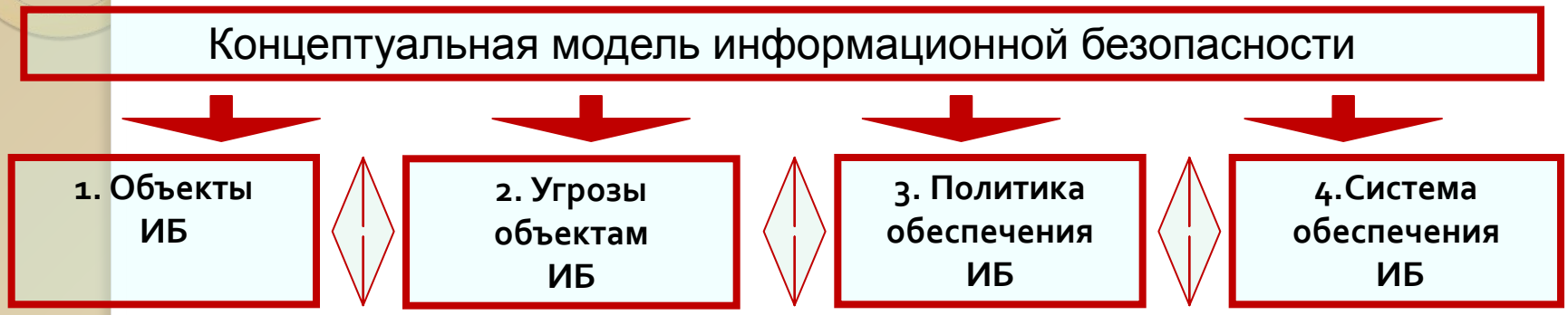
конфиденциальность информации - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

целостность информации - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

доступность информации - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно .

Информационная безопасность — это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры

КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Признак класса	Вид угрозы	Характеристика
1. По источнику угрозы	***Объективные*** *(Естественные)*	угрозы, вызванные воздействиями на системы обработки информации и ее компоненты объективных физических ***процессов*** или стихийных природных **явлений**, независящих от человека.
	Субъективные *(Искусственные)*	угрозы, вызванные умышленными или неумышленными действия ми человека
2. По отношению к объекту защиты	***Внутренние***	источник которых, расположен в пределах контролируемой зоны (территории, помещения)
	Внешние	источник которых, расположен вне контролируемой зоны (территории , помещения)
	Случайные	вызванные ошибками или халатностью персонала (непреднамеренные воздействия)
	Преднамеренные	вызванные целенаправленными действиями людей

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Признак класса	Вид угрозы	Характеристика
4. По цели действия	***Угроза конфиденциальности***	разглашение, НСД, получение разведками
	Угроза целостности	искажение (модификация), уничтожение, копирование
	Угроза доступности	блокирование доступа к информации или носителю
	Угроза праву собственности на информацию	несанкционированное тиражирование и распространение объектов интеллектуальной собственности
	Активные (атаки)	которые, при воздействии, вносят изменения в структуру и содержание АС («троянский конь» и др.)
	Пассивные	которые при реализации ничего не меняют в структуре и содержании АС (угроза копирования секретных данных)
	Материальный	потеря упущенной выгоды в результате разглашения коммерческой тайны, утраты интернет - ресурса.
	Моральный	(политический, личный, общественный)

Методы и средства обеспечения безопасности

Виды защиты	Определение	Сфера действия
Правовая защита информации	Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.	Территория государства, территория охватываемая международными соглашениями в области информационной безопасности
Организационная защита информации	**Организация деятельности по защите, регламентировании доступа к защищаемым ресурсам и на объекты информатизации**	Территория организации (предприятия) или объекта информатизации.
Техническая защита информации ***Инженерно-техническая*** ***Программно - аппаратная***	Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.	*Контролируемая зона, здание или помещение объекта информатизации (выделенное помещение)* *Масштаб: от одного отдельного компьютера до вычислительной сети (ЛВС)*
Криптографическая защита информации	**Защита информации с помощью ее криптографического преобразования.**	Масштаб сети (канала) связи, ИТКС (от организации до глобальной сети)
Физическая защита информации	Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.	Контролируемая зона, здание или помещение объекта информатизации (выделенное помещение)

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ (Общие понятия)

- Информационные ресурсы, содержащие сведения, связанные с государственной тайной и конфиденциальной информацией.

- Технические средства приёма, обработки и хранения информации (ТСПИ) — это средства вычислительной техники, сети и системы, программные средства (операционные системы, системы управления базами данных, прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приёма, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звуковоспроизведение, переговорные и телевизионные устройства, средства изготовления, тиражирование документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), т.е. системы и средства, непосредственно обрабатывающие конфиденциальную информацию и информацию, относящуюся к категории государственной тайны. .

ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ (Общие понятия)

- Технические средства и системы, не входящие в состав ТСПИ, но территориально находящиеся в помещениях обработки секретной и конфиденциальной информации называются вспомогательными техническими средствами и системами (ВТСС). (технические средства телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, радиотрансляции, часофикации, средства и системы передачи данных в системе радиосвязи, контрольно-измерительная аппаратура, электробытовые приборы и т.д., а также сами помещения, предназначенные для обработки информации ограниченного распространения.

- ТСПИ можно рассматривать как систему, включающую стационарное оборудование, периферийные устройства, соединительные линии, распределительные и коммуникационные устройства, системы электропитания, системы заземления. Технические средства, предназначенные для обработки конфиденциальной информации, включая помещения, в которых они размещаются, представляют объект ТСПИ.

Классификация технических каналов утечки информации

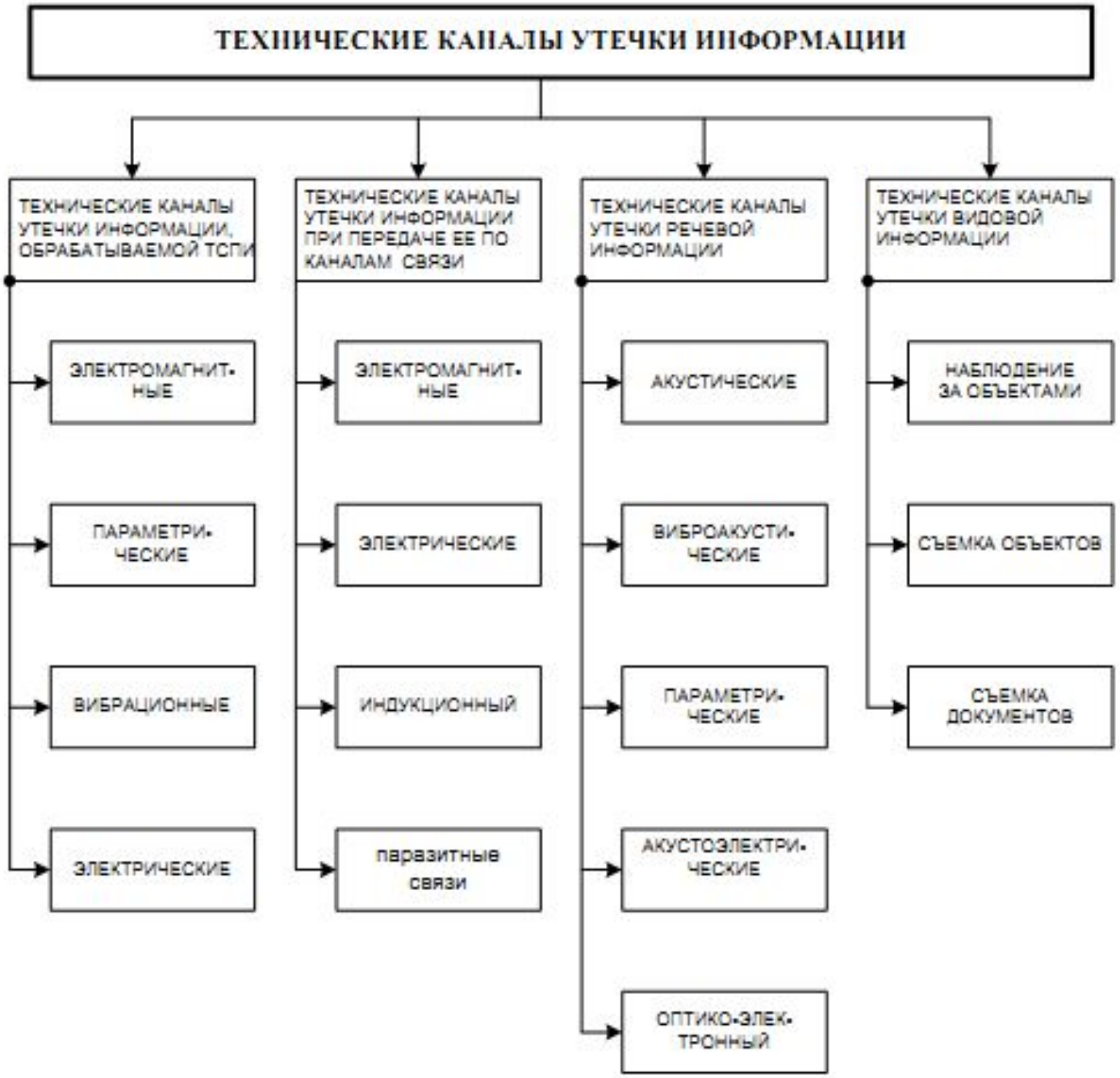
Утечка - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

Утечка (информации) по техническому каналу - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Технический канал утечки информации (ТКУИ), так же как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника. На приведена структура технического канала утечки информации.

Классификация технических каналов утечки информации

В качестве источника сигнала могут быть:

- объект наблюдения, отражающий электромагнитные и акустические волны;
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;
- передатчик функционального канала связи;
- закладное устройство;
- источник опасного сигнала;
- источник акустических волн, модулированных информацией.


ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ ТСПИ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ЕЕ ПО КАНАЛАМ СВЯЗИ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ РЕЧЕВОЙ ИНФОРМАЦИИ
ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ВИДОВОЙ ИНФОРМАЦИИ
ЭЛЕКТРОМАГНИТ-НЫЕ
ПАРАМЕТРИ-ЧЕСКИЕ
ВИБРАЦИОННЫЕ
ЭЛЕКТРИЧЕСКИЕ
ЭЛЕКТРОМАГНИТ-НЫЕ
ЭЛЕКТРИЧЕСКИЕ
ИНДУКЦИОННЫЙ
паразитные связи
АКУСТИЧЕСКИЕ
ВИБРОАКУСТИ-ЧЕСКИЕ
ПАРАМЕТРИ-ЧЕСКИЕ
АКУСТОЭЛЕКТРИ-ЧЕСКИЕ
ОПТИКО-ЭЛЕК-ТРОННЫЙ
НАБЛЮДЕНИЕ ЗА ОБЪЕКТАМИ
СЪЕМКА ОБЪЕКТОВ
СЪЕМКА ДОКУМЕНТОВ

Технические каналы утечки информации, обрабатываемой ТСПИ

1. Электромагнитные:
• электромагнитные излучения элементов ТСПИ;
• электромагнитные излучения на частотах работы ВЧ-генераторов ТСПИ;
• излучения на частотах самовозбуждения усилителей низкой частоты.
2. Электрические:
• наводки электромагнитных излучений элементов ТСПИ на посторонние проводники;
• просачивание информационных сигналов в линии электропитания;
• просачивание информационных сигналов в цепи заземления;
• съем информации с использованием закладных устройств.
3. Параметрические:
• перехват информации путем «высокочастотного облучения» ТСПИ.
4. Вибрационные:
• соответствие между распечатываемым символом и его акустическим образом.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы:

• электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

2. Электрические каналы:

• подключение к линиям связи.

3. Индукционный канал:

• эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

• паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки информации при передаче ее по каналам связи

1. Электромагнитные каналы:

• электромагнитные излучения передатчиков связи, модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных линий связи).

2. Электрические каналы:

• подключение к линиям связи.

3. Индукционный канал:

• эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов.

4. Паразитные связи:

• паразитные емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации.

Технические каналы утечки речевой информации

1. Акустические каналы:

• среда распространения – воздух.

2. Виброакустические каналы:

• среда распространения – ограждающие строительные конструкции.

3. Параметрические каналы:

• результат воздействия акустического поля на элементы схем, что приводит к модуляции высокочастотного сигнала информационным.

4. Акустоэлектрические каналы:

• преобразование акустических сигналов в электрические.

5. Оптико-электронный (лазерный) канал:

• облучение лазерным лучом вибрирующих поверхностей.

Технические каналы утечки видовой информации

1. Наблюдение за объектами.

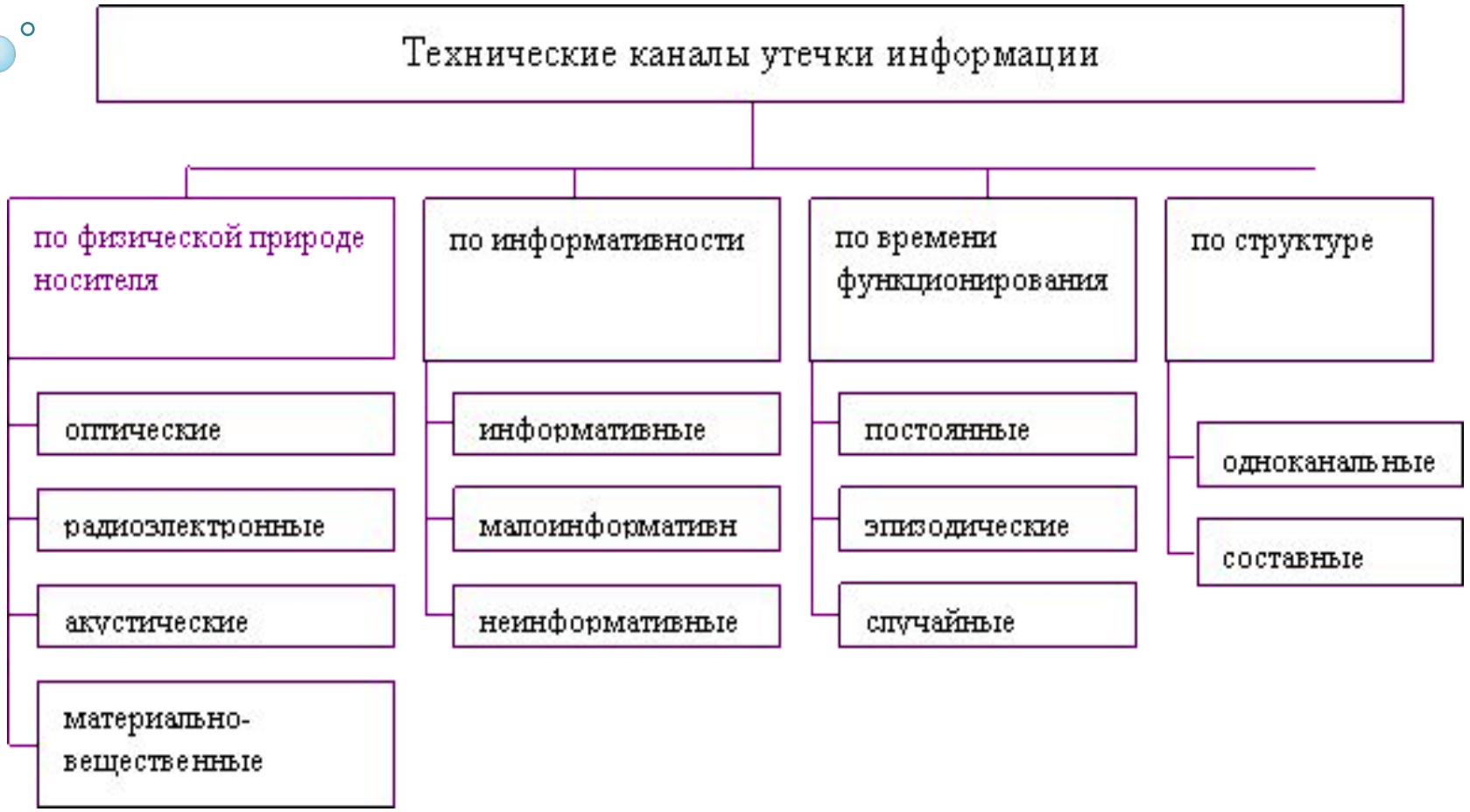
Для наблюдения днем применяются оптические приборы и телевизионные камеры. Для наблюдения ночью – приборы ночного видения, тепловизоры, телевизионные камеры.

2. Съемка объектов.

Для съемки объектов используются телевизионные и фотографические средства. Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи.

3. Съемка документов.

Съемка документов осуществляется с использованием портативных фотоаппаратов


Технические каналы утечки информации
по физической природе носителя
по информативности
по времени функционирования
по структуре
оптические
радиоэлектронные
акустические
материально-вещественные
информативные
малоинформативн
неинформативные
постоянные
эпизодические
случайные
одноканальные
составные

Классификация технических каналов утечки информации по физической природе носителя.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Оптический диапазон подразделяется на:

дальний инфракрасный поддиапазон 100 – 10 мкм (3 – 300 ТГц);

средний и ближний инфракрасный поддиапазон 10 – 0,76 мкм (30 – 400 ТГц);

видимый диапазон (сине-зелёно-красный) 0,76 – 0,4 мкм (400 – 750 Тгц).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот:

низкочастотный 10 – 1 км (30 – 300 кГц);

среднечастотный 1 км – 100 м (300 кГц – 3МГц);

высокочастотный 100 – 10 м (3 – 30 МГц);

ультравысокочастотный 10 – 1м (30 – 300 МГц);

и т.д. до сверхвысокочастотного 3 – 30 ГГц (10 – 1 см).

Классификация технических каналов утечки информации по физической природе носителя.

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Здесь различают:

инфразвуковой диапазон 1500 – 75 м (1 – 20 Гц);

нижний звуковой 150 – 5 м (1– 300 Гц);

звуковой 5 – 0,2 м (300 – 16000 Гц);

ультразвуковой от 16000 Гц до 4 МГц.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумаа.

Классификация технических каналов утечки информации по физической природе носителя.

Каналы утечки информации можно также классифицировать по информативности на информативные, малоинформативные и неинформативные. Информативность канала оценивается ценностью информации, которая передается по каналу.

По времени проявления каналы делятся на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. К эпизодическим каналам относятся каналы, утечка информации в которых имеет случайный разовый характер.

В результате реализации технических каналов утечки информации, возможно возникновение следующих угроз:

угроза утечки акустической информации;

угроза утечки видовой информации;

угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Классификация акустических каналов утечки информации

Информация, носителем которой являются акустические сигналы, называется акустической. Если источником информации является человеческая речь, ее называют речевой. Первичными источниками акустических колебаний являются механические системы, например, органы речи человека, а вторичными – преобразователи различного типа, в том числе электроакустические.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронный и параметрические

Классификация акустических каналов утечки информации

В **воздушных** акустических каналах утечки средой распространения акустических сигналов является воздух, а в качестве основного средства перехвата используется микрофон. Микрофон преобразует акустический сигнал в электрический и соединяется либо с записывающим устройством, либо с каким-то передатчиком. Передача полученных сигналов злоумышленнику может происходить по многим каналам: радиоканалу, оптическому каналу, по электросети и т.п.

Средой распространения акустических колебаний в **вибрационных** каналах являются конструкции зданий, стены, потолки, трубы и другие твердые тела. Для перехвата такой информации используются стетоскопы, в которых в качестве датчиков используются контактные микрофоны. Таким образом, электронные стетоскопы позволяют перехватывать информацию без доступа в защищаемые помещения.

Классификация акустических каналов утечки информации

Электроакустические каналы утечки информации возникают за счет электроакустических преобразований, то есть акустические сигналы преобразуются в электрические. Из окружающих нас устройств наиболее известны такие акустоэлектрические преобразователи, как системы звукового вещания, телефоны и микрофоны.

Оптико-электронный канал. Съем информации в таком канале реализуется с помощью лазера, поэтому иногда этот канал называют лазерным. Под действием звуковой волны тонкие отражающие поверхности, например, стекло или зеркало, начинают вибрировать. Если направить на них лазер, отраженное лазерное излучение модулируется и поступает на вход приемника оптического излучения. В приемнике полученный сигнал демодулируется и усиливается, и злоумышленник может получить исходный акустический сигнал.

Классификация акустических каналов утечки информации

Возникновение **параметрических каналов** обусловлено тем, что под давлением звуковой волны может измениться взаимное расположение элементов схем, проводов и т.п. в ВТСС и ОТСС. Вместе с расположением изменяются индуктивность и емкость. Соответственно, будет наблюдаться модуляция сигналов, проходящих через ВТСС и ОТСС, информационным сигналом, содержащимся в акустической волне. Промодулированные сигналы излучаются в пространство, где могут быть перехвачены средствами радиоразведки.

Если в помещении установлены полуактивные закладные устройства с элементами, параметры которых могут изменяться под действием акустической волны, возможен съем информации с помощью ВЧ-навязывания. Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленным излучением и приемник

Средства акустической разведки

По способу применения технические средства съема акустической информации можно подразделить на две большие категории:

1. средства, требующие физического проникновения в защищаемые помещения:
   радиозакладки;
   закладки с передачей акустической информации в ИК-диапазоне;
   закладки с передачей по сети 220 В;
   закладки с передачей информации по телефонной линии;
   диктофоны;
   проводниковые микрофоны;
   "телефонное ухо".

Средства акустической разведки

2. средства, не требующие физического проникновения в защищаемые помещения:

аппаратура, использующая "микрофонный эффект" устройств;

высокочастотное навязывание;

стетоскопы;

лазерные микрофоны;

направленные микрофоны.

Радиозакладки. Назначением этих устройств является передача по радиоканалу акустической информации с защищаемого объекта. Закладки могут быть исполнены в виде отдельного модуля или имитировать формой повседневные предметы обихода (пепельницу, зажигалку, калькулятор, авторучку и т.д.).