Лекция. Утечки информации. Классификация

- Определения понятия утечки информации
- Классификация видов утечки информации
- Средства и системы для обнаружения утечки информации

Утечки информации — неправомерная передача конфиденциальных сведений (материалов, важных для различных компаний или государства, персональных данных граждан), которая может быть умышленной или случайной. Любые сведения, находящиеся в компьютере, имеют свою стоимость. Поэтому похищение личных данных владельца компьютера способно нанести ему вред. Имея доступ к логинам и паролям, а также к банковским картам и счетам, злоумышленники крадут деньги граждан, промышленные секреты и тайны предприятий. Информация утекает в результате бесконтрольного распространения секретов за пределы кабинета, здания, предприятия. Утрата ценных сведений может случиться при неправильном использовании норм и правил политики безопасности. Несоблюдение правил защиты и хранения данных влекут за собой их утечку и распространение в общедоступных местах, таких как сеть «Интернет». Классификация видов утечки информации

Утечка информации возможна по разным причинам.

Умышленные утечки: Инсайдеры и избыточные права. К этому виду относятся случаи, основной причиной которых стали действия сотрудников, имеющих доступ к секретам легально, в силу своих служебных обязанностей.

Все варианты инсайда условно можно разделить на две группы: в одном случае сотрудник, не имея доступа к информации, получает ее незаконно, а в другом он обладает официальным доступом к закрытым данным и умышленно выносит их за пределы компании.

Кража информации (извне). Проникновение в компьютер с помощью вредоносных программ и похищение информации с целью использования в корыстных интересах. На хакерские атаки приходится 15% от всего объема утечек информации. Вторжение в устройство извне и незаметная установка вредоносных программ позволяют хакерам полностью контролировать систему и получать доступ к закрытым сведениям, вплоть до паролей к банковским счетам и картам. Для этого могут применяться различные программы вроде «троянских коней». *Главный атрибут данного вида утечки* — активные действия внешних лиц с целью доступа к информации.

Взлом программного обеспечения. Приложения, используемые в рабочем процессе или на личном компьютере сотрудника, часто имеют незакрытые уязвимости, которые можно эксплуатировать и получать тем самым различные небезопасные возможности вроде исполнения произвольного кода или повышения привилегий. Вредоносные программы (бекдоры, трояны) нацелены на причинение вреда владельцу устройства, позволяют незаметно проникать в систему и затем искажать или полностью удалять информацию, подменять ее другими, похожими данными. Кражи носителей. Весьма распространенный вариант утечек, который случается в результате преднамеренного хищения устройств с

информацией — ноутбуков, смартфонов, планшетов и других съемных носителей данных в виде флешек, жестких дисков.

Случайные утечки. К этому виду можно отнести инциденты, которые происходят из-за потери носителей данных (флешек, ноутбуков, смартфонов) или ошибочных действий сотрудников организации. Результатом может быть размещение конфиденциальной информации в интернете. Также не последнюю роль играет человеческий фактор, когда сотрудник по недосмотру открывает доступ к закрытым данным всем желающим. Анализ риска Для защиты от утечки конфиденциальной информации используются: системы аутентификации и идентификации, системы криптографической защиты дисковых данных, а также информации, передаваемой по сетям, программные решения для управления ключами шифрования. Средства аутентификации и идентификации позволяют ограничить доступ к ресурсам сети. Для этого у пользователя запрашивается некая информация, известная только ему, после чего открывается доступ. Для реализации этой возможности используются: биометрия — физиологические особенности людей (отпечатки пальцев, изображение радужной оболочки глаза и так далее); конфиденциальная информация — пароли, ключи и прочее. ***Для криптографической защиты информации применяются специальные средства***, помогающие маскировать содержимое данных. В результате шифрования преобразовывается каждый символ защищаемых сведений. Суть шифрования сводится к перестановке символов, замене, аналитическим преобразованиям или гаммированию. Распространены комбинированные средства шифрования, когда несколько различных методов используются поочередно.

Любые сведения, находящиеся в компьютере, *имеют свою стоимость*. Поэтому похищение личных данных владельца компьютера способно нанести ему вред. Имея доступ к логинам и паролям, а также к банковским картам и счетам, злоумышленники крадут деньги граждан, промышленные секреты и тайны предприятий. Информация утекает в результате бесконтрольного распространения секретов за пределы кабинета, здания, предприятия. *Утрата ценных сведений может случиться при неправильном использовании норм и правил политики безопасности*. Несоблюдение правил защиты и хранения данных влекут за собой их утечку и распространение в общедоступных местах, таких как сеть «Интернет». Классификация видов утечки информации Утечка информации возможна по разным причинам.

Каналы утечки информации — методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой [1, 2].

Играют основную роль в защите информации, как фактор информационной безопасности

Классификация

Все каналы утечки данных можно разделить на косвенные и прямые.

Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы.

Прямые соответственно требуют доступа к аппаратному обеспечению и данным информационной системы.

Примеры косвенных каналов утечки:

- Кража или утеря носителей информации, исследование не уничтоженного мусора;
- Дистанционное фотографирование, прослушивание;
- Перехват электромагнитных излучений.

Примеры прямых каналов утечки:

- Инсайдеры (*человеческий фактор*). Утечка информации вследствие несоблюдения коммерческой тайны;
- Прямое копирование.

Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования:

- акустические — запись звука, подслушивание и прослушивание;
- акустоэлектрические — получение информации через звуковые волны с дальнейшей передачей её через сети электропитания;
- виброакустические — сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- оптические — визуальные методы, фотографирование, видеосъемка, наблюдение;
- электромагнитные — копирование полей путём снятия индуктивных наводок;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съёма речевой информации «закладных устройств», модулированные информативным сигналом;
- материальные — информация на бумаге или других физических носителях информации

В зависимости от вида каналов связи технические каналы перехвата информации можно разделить[1]

- Перехват информации, передаваемой по каналам радио-, радиорелейной связи
    - Электромагнитный. Модулированные информационным сигналом высокочастотные электромагнитные излучения передатчиков средств связи могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования. Такой канал перехвата информации широко используется для прослушивания телефонных разговоров.
- Съем информации, передаваемой по кабельным линиям связи Канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры разведки к кабельным линиям связи.
    - Электрический. Часто используется для перехвата телефонных разговоров. При этом перехватываемая информация может непосредственно записываться на диктофон или передаваться по

радиоканалу в пункт приема для ее записи и анализа. Устройства, подключаемые к телефонным линиям связи и комплексированные с устройствами передачи информации по радиоканалу, часто называют телефонными закладками.

- Индукционный — канал перехвата информации, не требующий контактного подключения к каналам связи. При прохождении по кабелю информационных электрических сигналов вокруг кабеля образуется электромагнитное поле. Эти электрические сигналы перехватываются специальными индукционными датчиками. Индукционные датчики используются в основном для съёма информации с симметричных высокочастотных кабелей. Сигналы с датчиков усиливаются, осуществляется частотное разделение каналов, и информация, передаваемая по отдельным каналам, записывается на магнитофон или высокочастотный сигнал записывается на специальный магнитофон.

Технические каналы утечки информации можно разделить на естественные и специально создаваемые.

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).[2] 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.[2]

Технические каналы утечки информации

Акустический канал

Акустическая информация - информация, носителем которой является акустический сигнал.

Акустический сигнал - возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности. [3]

Различают первичные и вторичные акустические сигналы. К первичным относятся: сигналы, создаваемые музыкальными инструментами, пением, речью; шумовые сигналы, создаваемые для сопровождения различных музыкальных и речевых художественных передач (шум поезда, треск кузнечика и т. п.). Ко вторичным акустическим сигналам относятся сигналы, воспроизводимые электроакустическими устройствами, т. е. первичные сигналы, прошедшие по электроакустическим трактам связи и вещания и соответственно видоизмененные по своим параметрам.[4]

В зависимости от формы акустических колебаний различают простые (тональные) и сложные сигналы. Тональный - это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих. [5]

Виды технических каналов утечки акустической информации:[6]

Виды технических каналов утечки акустической информации	
Воздушные	Перехват сигналов микрофонами
	В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.
Электроакустические	Перехват колебаний через ВТСС(Вспомогательные технические средства и системы)
	Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС(Вспомогательные технические средства и системы)
Вибрационные	Перехват сигналов электронными стетоскопами
	В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).
Параметрические	Перехват сигналов путем приема и детектирования побочных ЭМИ (на частотах генератора высокой частоты(ВЧ)), ТСПИ(Технические средства приема информации) и ВТСС (Вспомогательные технические средства и системы)
	В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ТСПИ и ВТСС.

	При этом изменяется (незначительно) 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. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а, следовательно, к изменению частоты излучения генератора, т.е. к частотной модуляции сигнала. Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора.
Оптико-электронные (лазерный)	Перехват сигналов путем лазерного зондирования оконных стекол
	Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация. Причем лазер и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях).

Акустический канал утечки информации реализуется в следующем:

- подслушивание разговоров на открытой местности и в помещениях, находясь рядом или используя направленные микрофоны (бывают параболические, трубчатые или плоские). Направленность 2-5 градусов, средняя дальность действия наиболее распространенных — трубчатых составляет около 100 метров. При хороших климатических условиях на открытой местности параболический направленный микрофон может работать на расстояние до 1 км;
- негласная запись разговоров на диктофон или магнитофон (в том числе цифровые диктофоны, активизирующиеся голосом);
- подслушивание разговоров с использованием выносных микрофонов (дальность действия радиомикрофонов 50-200 метров без ретрансляторов).

Микрофоны, используемые в радиозакладках, могут быть встроенными или выносными и имеют два типа: акустические (чувствительные в основном к действию звуковых колебаний воздуха и предназначенные для перехвата речевых сообщений) и вибрационные (преобразующие в электрические сигналы колебания, возникающие в разнообразных жестких конструкциях).

Акустоэлектрический канал

Акустоэлектрический канал утечки информации, особенностями которого являются:

- удобство применения (электросеть есть везде);
- отсутствие проблем с питанием у микрофона;
- возможность съёма информации с питающей сети не подключаясь к ней (используя электромагнитное излучение сети электропитания). Прием информации от таких «жучков» осуществляется специальными приёмниками, подключаемыми к силовой сети в радиусе до 300 метров от «жучка» по длине проводки или до силового трансформатора, обслуживающего здание или комплекс зданий;
- возможные помехи на бытовых приборах при использовании электросети для передачи информации, а также плохое качество передаваемого сигнала при большом количестве работы бытовых приборов.

Предотвращение:

- трансформаторная развязка является препятствием для дальнейшей передачи информации по сети электропитания;

Виброакустический канал (телефонный)

Телефонный канал утечки информации для подслушивания телефонных переговоров (в рамках промышленного шпионажа) возможен:

- гальванический съем телефонных переговоров (путём контактного подключения подслушивающих устройств в любом месте абонентской телефонной сети). Определяется путём ухудшения слышимости и появления помех, а также с помощью специальной аппаратуры;
- телефонно-локационный способ (путём высокочастотного навязывания). По телефонной линии подается высокочастотный тональный сигнал, который воздействует на нелинейные элементы телефонного аппарата (диоды, транзисторы, микросхемы) на которые также воздействует акустический сигнал. В результате в телефонной линии формируется высокочастотный модулированный сигнал. Обнаружить подслушивание возможно по наличию высокочастотного сигнала в телефонной линии. Однако дальность действия такой системы из-за затухания ВЧ сигнала в двухпроводной линии не превышает ста метров. Возможное противодействие: подавление в телефонной линии высокочастотного сигнала;
- индуктивный и ёмкостной способ негласного съёма телефонных переговоров (бесконтактное подключение).

Индуктивный способ — за счёт электромагнитной индукции, возникающей в процессе телефонных переговоров вдоль провода телефонной линии. В качестве приемного устройства съёма информации используется трансформатор, первичная обмотка которого охватывает один или два провода телефонной линии.

Ёмкостной способ — за счет формирования на обкладках конденсатора электростатического поля, изменяющегося в соответствии с изменением уровня телефонных переговоров. В качестве приёмника съёма телефонных переговоров используется ёмкостной датчик, выполненный в виде двух пластин, плотно прилегающих к проводам телефонной линии.

Подслушивание разговоров в помещении с использованием телефонных аппаратов возможно следующими способами:

- низкочастотный и высокочастотный способ съёма акустических сигналов и телефонных переговоров. Данный способ основан на подключении к телефонной линии подслушивающих устройств, которые преобразованные микрофоном звуковые сигналы передают по телефонной линии на высокой или низкой частоте. Позволяют прослушивать разговор как при поднятой, так и при опущенной телефонной трубке. Защита осуществляется путём отсекания в телефонной линии высокочастотной и низкочастотной составляющей;
- использование телефонных дистанционных подслушивающих устройств. Данный способ основывается на установке дистанционного подслушивающего устройства в элементы абонентской телефонной сети путём параллельного подключения его к телефонной линии и дистанционным включением. Дистанционное телефонное подслушивающее устройство имеет два деконспирирующих свойства: в момент подслушивания телефонный аппарат абонента отключён от телефонной линии, а также при положенной телефонной трубке и включённом подслушивающем устройстве напряжение питания телефонной линии составляет менее 20 Вольт, в то время как она должна составлять 60.

Оптический канал

Каналы утечки информации, передаваемой по оптическим линиям связи

В оптическом канале получение информации возможно путём:

- визуального наблюдения,
- фото-видеосъемки,
- использования видимого и инфракрасного диапазонов для передачи информации от скрыто установленных микрофонов и других датчиков.

В качестве среды распространения в оптическом канале утечки информации выступают:

- безвоздушное пространство;
- атмосфера;
- оптические световоды.

Безвоздушное пространство, являющееся средой распространения утечки информации, возникает при наблюдении за наземными объектами с космических аппаратов. К свойствам среды распространения, влияющих на длину канала утечки, относятся:

- характеристики прозрачности среды распространения;
- спектральные характеристики света.

Типовые варианты оптических каналов утечки информации приведены в таблице.

Объект наблюдения	**Среда распространения**	**Оптический приемник**
Человек в помещении	Воздух	Глаза человека+бинокль

Во дворе, на улице	Воздух+стекло	Фото, кино, телев. ап-ра

Технические средства промышленного шпионажа

Подслушивающее устройство

- средства акустического контроля;
- аппаратура для съёма информации с окон;
- специальная звукозаписывающая аппаратура;
- микрофоны различного назначения и исполнения;
- электросетевые подслушивающие устройства;
- приборы для съёма информации с телефонной линии связи и сотовых телефонов;
- специальные системы наблюдения и передачи видеоизображений;
- специальные фотоаппараты;
- приборы наблюдения в дневное время и приборы ночного видения;
- специальные средства радиоперехвата и приёма.

Технические средства съёма информации могут быть внедрены «противником» следующими способами:

- установка средств съёма информации в ограждающие конструкции помещений во время строительных, ремонтных и реконструкционных работ;
- установка средств съёма информации в предметы мебели, другие предметы интерьера и обихода, различные технические средства как общего назначения, так и предназначенные для обработки информации;
- установка средств съёма информации в предметы обихода, которые вручаются в качестве подарков, а впоследствии могут использоваться для оформления интерьера служебных помещений;
- установка средств съёма информации в ходе профилактики инженерных сетей и систем. При этом в качестве исполнителя могут быть использованы даже сотрудники ремонтных служб.

Средства и системы для обнаружения утечки информации

Любой злоумышленник оставляет следы, даже на уровне передачи невидимых сигналов. Техническое устройство изменяет окружающее пространство. Главная цель разведки – добиться того, чтобы устройства, формирующие канал утечки информации, не были обнаружены как можно дольше.

А задача контрразведки заключается в том, чтобы быстро зафиксировать и найти место утечки информации. Сложность этого процесса в том, что неизвестно, какое именно устройство использует злоумышленник. Чтобы выяснить методику получения данных незаконным путем, важно проследить за всеми направлениями и способами получения информации. Нельзя останавливаться на одном методе, требуется проводить контрразведку комплексно.

Вычисление утечки информации

Технические средства для разведки и обезвреживания каналов утечки информации можно определить следующим образом:

1. Активный тип поисковых работ:

- Нелинейные локаторы (они откликаются при обнаружении электромагнитного поля).
- Рентгенметры (происходит вычисление канала путем просвечивания с помощью рентгеновских излучений).
- МРЛ (магнитно-резонансные устройства определяют посторонние вмешательства по молекулам в магнитном поле).
- С помощью акустических коррелятоpов.

2. Пассивный способ обнаружения утечки проходит с помощью:

- Металлоискателей.
- Тепловизоров.
- Приборов по изменению всех показателей телефонной линии (индукции, напряжения, емкости).
- Девайсов, которые изменяют параметры магнитного поля.
- Систем поисков электромагнитных излучений с посторонними сигналами.

Не все методики можно применить в современных условиях. Выбор способа происходит по требованиям контрразведки. Например, рентгеновские аппараты – громоздкие, поэтому их невозможно транспортировать или применять оперативно в военно-полевых условиях. Такие же недостатки есть у магнитно-резонансных локаторов, поэтому они используются в крупных компаниях стационарно.

Одно из самых прогрессивных направлений разведки и защиты информации от утечки – использование тепловизоров. Приборы дорогостоящие, но мобильные и обладают высокой чувствительностью. Они могут регистрировать сигналы мощностью 1 мкВт. А принцип действия основан на выделении тепла любым техническим устройством.

На сегодня чаще всего используются электромагнитные локаторы разной конфигурации:

- Приемники.
- Шумоизмерители.
- Детекторы инфракрасных излучений.
- Анализаторы спектра.
- Измерители частот и панорамные устройства.

Общим для всех этих устройств является то, что их задача состоит в выделении сигнала передатчика.

Существуют приборы, которые делают анализ телефонной линии благодаря применению нелинейной локации, но они не используются в широких массах из-за сложности настройки и получения неоднозначных результатов.

Важно уделить достаточное внимание защите от подключения посторонних технических каналов утечки. Можно обезопасить связь от индуктивных наводок и предотвратить утечку охраняемой информации с помощью генераторов шума. Устройство можно использовать в телефоне, оно зашумляет телефонные линии, которые были совместно проложены, во всех диапазонах звуковых частот.

Такая простая методика или поможет владельцу телефона и остановит несанкционированную передачу информации, или как минимум усложнит задачу мошеннику. Эффективность будет наблюдаться в любом случае.

Возникновение технических каналов утечки информации – не редкость, поэтому важно знать о них больше для того, чтобы защитить себя и свою конфиденциальность в разговорах или в момент передачи сообщения.

Способы защиты информации

Правовые

Защита информации от утечки по техническим каналам осуществляется на основе конституций и законов, а также защита обеспечивается наличием авторских свидетельств, патентов, товарных знаков.[7]

В России существует стандарт, который устанавливает классификацию и перечень факторов, воздействующих на защищаемую информацию, в интересах обоснования требований защиты информации на объекте информатизации. Настоящий стандарт распространяется на требования по организации защиты информации при создании и эксплуатации объектов информатизации, используемых в различных областях деятельности (обороны, экономики, науки и других областях).[8] Требование соблюдения законов Российской Федерации, в частности “Об информации, информационных технологиях и о защите информации” [9], “О государственной тайне”[10], “О коммерческой тайне”[11] и других законодательных актов Российской Федерации:

«Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утверждённого Постановлением Правительства РФ от 15.09.93 № 912-51[12], «Положения о лицензировании деятельности предприятий, организаций и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»[13], утвержденного Постановлением Правительства РФ от 15 апреля 1995 г. № 333, “Положения о государственном лицензировании деятельности в области защиты информации”, утвержденного Постановлением Правительства РФ от 27 апреля 1994 г. № 10[14], «Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации», утверждённого Постановлением Правительства РФ от 27 мая 2002 г. № 348, с изменениями и дополнениями от 3 октября 2002 г. № 731[15], «Положения о сертификации средств защиты информации», утверждённого Постановлением Правительства РФ от 26 июня 1995 г. № 608[16], Постановлений Правительства Российской Федерации «О лицензировании деятельности по технической защите конфиденциальной информации» (от 30 апреля 2002 г. № 290, с изменениями и дополнениями от 23 сентября 2002 г. № 689 и от 6 февраля 2003 г. № 64)[17], «О лицензировании отдельных видов деятельности» (от 11 февраля 2002 г. № 135)[18], а также “Положения по аттестации объектов информатизации по требованиям безопасности информации”, утвержденного Председателем Гостехкомиссии России 25 ноября 1994 г.[19], и других нормативных документов.

Организационные

Обеспечивается совокупностью положений о Службе безопасности и планами работы этой службы. Планы мероприятий службы безопасности охватывают широкий круг вопросов, в частности:

а) на ранней стадии при проектировании помещений и строительстве Служба безопасности рассматривает следующие вопросы: выделение помещений для совещаний и переговоров (в таком помещении делается специальные перекрытия и каналы воздушной вентиляции, отдельные комнаты экранируют и так далее); удобство контроля помещений, людей, транспорта; создание производственных зон по типу конфиденциальности работ с самостоятельным дополнительным допуском;[7]

б) служба безопасности участвует в подборе персонала с проверкой их качеств на основании личных бесед (изучение трудовой книжки, получения информации с других мест работы; затем принимаемый на работу ознакомляется с правилами работы с конфиденциальной информацией и порядком ответственности);[7]

в) служба безопасности готовит положения и осуществляет: организацию пропускного режима; организацию охраны помещений и территорий; организацию хранения и использования документов, порядок учета, хранения, уничтожения документов, плановые проверки.[7]

Инженерно-технические

Защита включает в себя: аппаратные средства защиты; программные средства защиты – это использование специальных программ в системах, средствах и сетях обработки данных; математические способы защиты – применение математических и криптографических методов в целях защиты конфиденциальной информации (без знания ключа невозможно узнать и дешифровать украденную информацию).[7]

1. Хорев А.А. "Защита информации от утечки по техническим каналам"часть1 Технические каналы утечки информации" (недоступная ссылка). www.analitika.info. Дата обращения: 21 ноября 2017. Архивировано 16 ноября 2017 года.
2. ↑ Перейти обратно:1 2 Раздел статьи по Защите Информации и Безопасности (недоступная ссылка). www.analitika.info. Дата обращения: 21 ноября 2017. Архивировано 1 декабря 2017 года.
3. ↑ Безопасность информационных технологий. Методология создания систем защиты - Украинский Центр Информационной Безопасности (недоступная ссылка). www.bezpeka.com. Дата обращения: 21 ноября 2017. Архивировано 21 апреля 2018 года.
4. ↑ Электроакустика (Сапожков М. А.). know.sernam.ru. Дата обращения: 21 ноября 2017.
5. ↑ Хорев А.А. "Защита информации от утечки по техническим каналам"часть1 Технические каналы утечки информации" (недоступная ссылка). www.analitika.info. Дата обращения: 21 ноября 2017. Архивировано 1 декабря 2017 года.
6. ↑ Хорев А.А. "Защита информации от утечки по техническим каналам"часть1 Технические каналы утечки информации" (недоступная ссылка). www.analitika.info. Дата обращения: 21 ноября 2017. Архивировано 1 декабря 2017 года.
7. ↑ Перейти обратно:1 2 3 4 5 Технические средства защиты информации: Учебное пособие. Читать бесплатно онлайн в электронном виде | Единое окно. window.edu.ru. Дата обращения: 21 ноября 2017.

8. ↑ *znaytovar.ru*. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. znaytovar.ru. Дата обращения: 23 ноября 2017.
9. ↑ Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.11.2017) / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
10. ↑ Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне" / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
11. ↑ Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне» / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
12. ↑ Постановление Совета Министров - Правительства РФ от 15.09.1993 № 912-51 «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от её утечки по техническим каналам» - Нормативные. artiks.ru. Дата обращения: 23 ноября 2017.
13. ↑ О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием.... pravo.gov.ru. Дата обращения: 23 ноября 2017.
14. ↑ ПОЛОЖЕНИЕ О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
15. ↑ Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 15.06.2016) «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» (вместе с "Положением о лицензировании деятельности по разработке и / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
16. ↑ Положение о сертификации средств защиты информации по требованиям безопасности информации, Приказ Гостехкомиссии России от 27 октября 1995 года №199. docs.cntd.ru. Дата обращения: 23 ноября 2017.
17. ↑ Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
18. ↑ Федеральный закон от 04.05.2011 N 99-ФЗ (ред. от 29.07.2017) "О лицензировании отдельных видов деятельности" / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.
19. ↑ «Положение по аттестации объектов информатизации по требованиям безопасности информации» (утв. Гостехкомиссией РФ 25.11.1994) / КонсультантПлюс. www.consultant.ru. Дата обращения: 23 ноября 2017.