Ответы на вопросы к экзамену по ИБ

## 1. Понятие «информации» в области информационной безопасности (данные, сообщения, сведения).

**Информация** - сведения (данные, сообщения) независимо от формы их представления.

Данные - информация, представленная на материальном носителе в виде букв, цифр, символов и т.д.

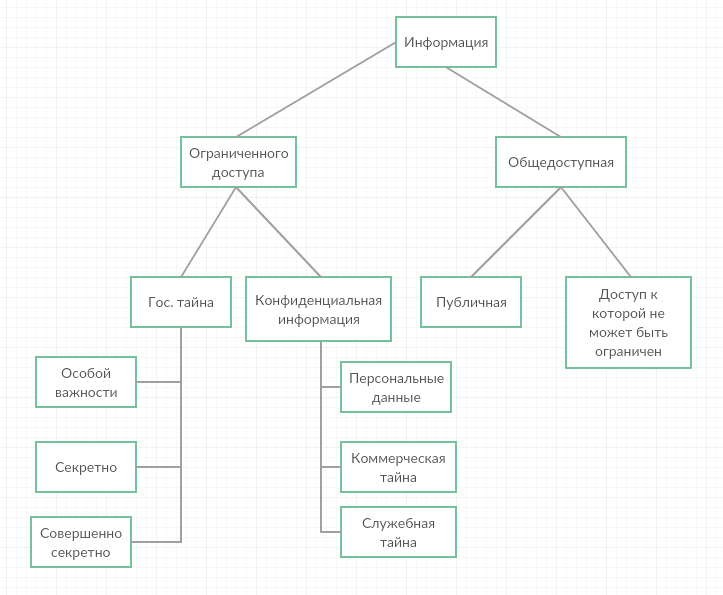
Сообщение – данные, передаваемые по «каналу связи» с использованием различных сигналов. *«Канал связи» - совокупность передатчика сигнала, среды его распространения и приемника сигнала. Сигнал – материальный носитель информации, используемый для передачи сообщений в системе связи.*

Сведения – смысловое содержание данных, сформированное сознанием человека с помощью смысловых образов.

Информация бывает объективная (данные, сообщение) и субъективная (сведения).

## 2. Виды защищаемой информации.

**Защищаемая информация** – это информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.



Сведения особой важности – распространение может нанести ущерб интересам РФ в одной или нескольких областей (военной, внешнеполитической, экономической и т.д.)

Совершенно секретные сведения – распространение может нанести ущерб интересам министерств или отрасли экономики РФ в одной или нескольких областей (военной, внешнеполитической, экономической и т.д.)

Секретные сведения – все иные сведения из числа государственной тайны.

## 3. Свойства информации. Безопасность информации (определение).

**Информация** - сведения, данные, сообщения независимо от формы их представления.

Свойства:

* Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
* Доступность - состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.
* Целостность - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

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

## 4. Классификация угроз конфиденциальности сообщений (перехват информации, утечка информации по техническим каналам). Ответственность за перехват информации.

**Угрозы конфиденциальности сообщений (неправомерное получение сообщений)**

* Перехват сообщений техническими средствами
* утечка информации по техническим каналам.

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

**Утечка информации по техническому каналу:** неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

**Утечка информации –** неконтролируемое распространение защищаемой информации, вследствие ее разглашения, хищения, копирования, несанкционированного доступа, а также перехвата информации техническими средствами.

**Статья 272. Неправомерный доступ к компьютерной информации**

 1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - наказывается штрафом в размере **до двухсот тысяч рублей** или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, - наказывается штрафом в размере **от ста тысяч до трехсот тысяч** рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

 3. Деяния, предусмотренные ч. 1 или ч. 2 настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные ч. 1, ч. 2 иди ч. 3 настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания.

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

**5. Классификация угроз конфиденциальности данных (хищение данных, несанкционированный доступ к данным, несанкционированное копирование данных). Ответственность за несанкционированный доступ к данным.**

Угрозы конфиденциальности данных (неправомерное получение данных)

1. Хищение носителя информации.

**Кража** - тайное хищение носителей информации.

**Грабеж** - открытое хищение носителей информации.

**Разбой** - нападение с целью хищения носителя информации, совершенном с применением насилия, опасного для жизни и здоровья, либо с угрозой применения такого насилия.

1. Несанкционированное копирование данных с носителя.
2. Несанкционированный доступ к данным, обрабатываемым АС.

**Несанкционированный доступ к информации** - доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации с применением штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС), или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

*Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.*

**Ответственность – см. вопрос 2 ст.272**

**6. Угрозы целостности и доступности информации. Причины непреднамеренного несанкционированного воздействия на информацию. Виды несанкционированного преднамеренного воздействия на информацию.**

**Угрозы целостности информации**

**Угрозы целостности сведений:**

* Физическое устранение человека.
* Изменение сознания под воздействием средств психологического, психофизиологического, технического, информационного воздействия и т.д.
* «Стирание» или повреждение памяти.
* Формирование «требуемого» сознания («зомби»)

**Угрозы целостности данных**

* Модифицирование данных (искажение, подмена).
* Уничтожение или повреждение данных.

**Угрозы целостности сообщений:**

* Модифицирование сообщений (искажение, подмена (передача ложных сообщений) ).
* Подавление сигналов при их передаче по каналам связи.

**Угрозы доступности информации**

**Угрозы доступности сведений**

* Изменение сознания под воздействием средств психологического, психофизиологического, технического, информационного воздействия и т.д. , при котором невозможно получить сведения, которыми обладал человек.
* «Стирание» или повреждение памяти.

**Угрозы доступности данных**

* Блокирование доступа к данным
* Навязывание «ложной информации», затрудняющей доступ к достоверной информации.
* Распространение огромного количества «ненужной» информации, затрудняющей поиск требуемой информации и т.д.

**Угрозы доступности сообщений**

* Отключение элементов информационных и телекоммуникационных систем (ИТКС).
* Огневое поражение элементов ИТКС.
* Радиоэлектронное, оптикоэлектронное подавление и поражение ИТКС.
* Программно-математическое воздействие на ИТКС (например, кибератаки).
* Программно-техническое воздействие на ИТКС (например, закладочные устройства) и т.д.

Причины **непреднамеренного несанкционированного воздействия на информацию**:

* природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды и т.д.);
* непреднамеренные электромагнитное или радиоционное облучение технических средств обработки информации (ТСОИ) и носителей информации;
* дефекты, сбои, отказы, аварии ТСОИ;
* дефекты, сбои и отказы программного обеспечения ТСОИ;
* дефекты, сбои, отказы, аварии систем и средств обеспечения ТСОИ;
* ошибки обслуживающего персонала объекта информатизации (ошибки при эксплуатации ТСОИ и программных средств ТСОИ, ошибки при эксплуатации средств и систем защиты информации) и т.д.

**Преднамеренные угрозы целостности и доступности информации**:

* использование специальных программных (программнно-математических) воздействий на информацию и программное обеспечение ТСОИ;
* использование специальных программно-технических воздействий на информацию, ТСОИ и программное обеспечение;
* преднамеренное силовое электромагнитное воздействие на информацию, ТСОИ и носители информации;
* диверсии в отношении объекта информатизации и т.д.

**7. Угроза безопасности информации (определение). Классификация угроз безопасности информации. Классификация источников угроз безопасности информации.**

**Угроза безопасности информации −** совокупность факторов (явлений, действий или процессов) и условий их реализации, результатом которых могут быть утечка, неправомерные модифицирование (искажение, подмена), уничтожение информации или блокирование доступа к ней.

**Классификация угроз безопасности информации**

* угрозы конфиденциальности информации
* угрозы целостности информации
* угрозы доступности информации

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

**Источники угрозы безопасности информации**

**1. Внешние угрозы**:

- деятельность специальных служб иностранных государств,

- деятельность преступных сообществ, организаций и групп,

- противозаконная деятельность отдельных лиц.

**2. Внутренние угрозы**:

- нарушение установленного регламента сбора, обработки и передачи информации,

- преднамеренные действия и ошибки персонала ОИ,

- отказ технических средств и сбои программного обеспечения ТСОИ.

**8. Классификация угроз конфиденциальности сведений (разглашение сведений ограниченного доступа, неправомерный доступ к сведениям ограниченного доступа). Ответственность за разглашение сведений ограниченного доступа и неправомерный доступ к сведениям ограниченного доступа.**

**Угрозы конфиденциальности сведений**

* Разглашение сведений ограниченного доступа - противоправное предание огласке сведений ограниченного доступа, при котором они стали достоянием посторонних лиц.

**Разглашение сведений ограниченного доступа**:

* **преднамеренное** (при прямом умысле);

**Действия, в результате которых осуществляется *преднамеренное* разглашение сведений ограниченного доступа:**

* разговор с посторонними лицами по закрытой тематике;
* ознакомление посторонних лиц с информацией ограниченного доступа, содержащейся на различного вида носителях, в том числе и электронных (без передачи носителя информации постороннему лицу);
* передача носителя информации, содержащего сведения ограниченного доступа, постороннему лицу (в том числе по каналу связи, включая Интернет);
* публичное выступление;
* публикации в средствах массовой информации;
* распространение сведений через Интернет и т.п.
* **непреднамеренное** (по неосторожности).

**Действия, в результате которых может произойти *непреднамеренное* разглашение сведений ограниченного доступа:**

* утрата носителя информации, содержащего сведения ограниченного доступа;
* копирование информации на незарегистрированный носитель информации;
* разговор по закрытой тематике вне выделенных или защищаемых помещений;
* обработка информации ограниченного доступа на незащищенных технических средствах (автоматизированных системах);
* обработка информации ограниченного доступа (ведение конфиденциальных переговоров) при выключенных (отключенных) или неисправных технических средствах защиты;
* передача информации ограниченного доступа по незащищенным каналам связи;
* вынос носителей информации ограниченного доступа за пределы контролируемой зоны объекта;
* оставление документов, электронных носителей информации, содержащих сведения ограниченного доступа, в условиях, когда с ними могут ознакомиться посторонние лица (например, оставление документов на рабочем столе при выходе из помещения, хранение носителей информации вне специального сейфа т.п.).
* обработка информации ограниченного доступа на СВТ в условиях, когда посторонние лица могут осуществлять чтение информации с экрана монитора или чтение распечаток документов (например, обработка информации в присутствии уборщицы, оставление СВТ в режиме вывода конфиденциальной информации на экран монитора при выходе из помещения и т.д.).
* Неправомерное получение сведений

**Неправомерное предоставление информации** – противоправное предание огласке сведений ограниченного доступа, при котором они стали достоянием *определенного* круга посторонних лиц.

**Неправомерное распространение информации** – противоправное предание огласке сведений ограниченного доступа, при котором они стали достоянием *неопределенного* круга посторонних лиц.

**Статья 283. Разглашение государственной тайны**

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, если эти сведения стали достоянием других лиц, при отсутствии признаков преступлений, предусмотренных ст 275 и 276 настоящего Кодекса, - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

**Статья 275. Государственная измена**

Государственная измена, то есть совершенные гражданином Российской Федерации шпионаж, выдача иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, доверенную лицу или ставшую известной ему по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, - наказывается лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет.

**9. Классификация угроз целостности информации (сведений, данных и сообщений). Ответственность за нарушение целостности информации.**

**Угрозы целостности сведений:**

* Физическое устранение человека.
* Изменение сознания под воздействием средств психологического, психофизиологического, технического, информационного воздействия и т.д.
* «Стирание» или повреждение памяти.
* Формирование «требуемого» сознания («зомби»)

**Угрозы целостности данных**

* Модифицирование данных (искажение, подмена).
* Уничтожение или повреждение данных.

**Угрозы целостности сообщений:**

* Модифицирование сообщений (искажение, подмена (передача ложных сообщений) ).
* Подавление сигналов при их передаче по каналам связи.

**10. Классификация угроз доступности (сведений, данных и сообщений). Ответственность за нарушение доступности информации.**

**Угрозы доступности сведений**

* Изменение сознания под воздействием средств психологического, психофизиологического, технического, информационного воздействия и т.д. , при котором невозможно получить сведения, которыми обладал человек.
* «Стирание» или повреждение памяти.

**Угрозы доступности данных**

* Блокирование доступа к данным
* Навязывание «ложной информации», затрудняющей доступ к достоверной информации.
* Распространение огромного количества «ненужной» информации, затрудняющей поиск требуемой информации и т.д.

**Угрозы доступности сообщений**

* Отключение элементов информационных и телекоммуникационных систем (ИТКС).
* Огневое поражение элементов ИТКС.
* Радиоэлектронное, оптикоэлектронное подавление и поражение ИТКС.
* Программно-математическое воздействие на ИТКС (например, кибератаки).
* Программно-техническое воздействие на ИТКС (например, закладочные устройства) и т.д.

**11. Защита информации (определение). Направления защиты информации (организационно-правовая защита информации, техническая защита информации, криптографическая защита информации, физическая защита объектов информатизации). Ответственность за незаконную деятельность по защите информации и нарушение правил защиты информации.**

**Защита информации** – принятие организационно-правовых, технических, криптографических и физических мер, направленных на обеспечение безопасности информации.

* Организационно - правовая защита информации – защита информации правовыми методами, включает в себя разработку законодательных и нормативных правовых документов и организационно-распорядительных документов, применение этих документов, а также надзор и контроль за их исполнением.
* Техническая защита информации – защита информации, заключается в обеспечении некриптографическими методами безопасности информации, подлежащей защите, с применением технических, программных и программно-технических средств.

**Техническая защита информации:**

* защита информации от несанкционированного доступа и неправомерного воздействия на информацию (защита от НСД);
* защита информации от утечки по техническим каналам.
* Криптографическая защита информации – защита информации с помощью ее криптографического преобразования с использованием технических, программных и программно-технических средств.
* Физическая защита информации **– з**ащита информации путем применения организационных мероприятий и средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

**КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ (30 декабря 2001 года N 195-ФЗ)**

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), -твлечет наложение административного штрафа на граждан в размере от одной тысячи до одной тысячи пятисот рублей;

на должностных лиц - от одной тысячи пятисот до двух тысяч пятисот рублей;

на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), -

влечет наложение административного штрафа

на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой;

на должностных лиц - от двух тысяч пятисот до трех тысяч рублей;

на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, -

влечет наложение административного штрафа

на должностных лиц в размере от двух тысяч до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей.

(в ред. Федеральных законов от 22.06.2007 [N 116-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_155176/?dst=100505), от 02.12.2013 [N 341-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_155128/?dst=100012))

**Продолжение – см. лекция 2 слайд 32 и до конца**

**12.Задачи защиты информации.**

1. Защита объектов информатизации (ОИ) от утечки информации по техническим каналам.
2. Защита выделенных помещений (ВП) от утечки речевой информации по техническим каналам.
3. Защита АС от несанкционированного доступа к информации.
4. Защита информации и программного обеспечения от специальных программных воздействий, вызывающих уничтожение, искажение информации, блокирование доступа к ней или сбои в работе ТСОИ (технических средств обработки информации).
5. Выявление электронных устройств перехвата информации, несанкционированно внедренных в ТСОИ и ВП.
6. Защита информации, передаваемой по каналам связи.
7. Защита носителей информации от несанкционированного копирования.
8. Обеспечение режима секретности (конфиденциальности) информации.
9. Физическая защита объектов и носителей информации.
10. Защита носителей информации и ТСОИ от преднамеренного силового электромагнитного воздействия, вызывающих разрушение носителей информации или ТСОИ или сбои в их работе.
11. Защита носителей информации от утраты.

**13.Несанкционированный доступ к информации (определение). Классификация способов НСД к информации (программно-технический, программный). Угрозы безопасности информации на сетевом уровне.**

**Несанкционированный доступ к информации** - доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации с применением штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС), или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Способы несанкционированного доступа (НСД):

* программно-технический

**При программно-техническом (физическом) доступе** нарушитель осуществляет несанкционированное вскрытие системного блока СВТ и изъятие HDD или изменение аппаратной части СВТ.

**Средства копирования носителей информации**

Talon Enhanced, SuperSonix

* программный

При **программном доступе** нарушитель использует программное обеспечение, позволяющие реализовать НСД к информации без вскрытия системного блока или изменения аппаратной части СВТ.

**Способы несанкционированного доступа** **с использованием программных средств** :

* маскировка под зарегистрированного пользователя;
* непосредственное обращение к объектам доступа;
* использование программных средств, выполняющих обращение к объектам доступа в обход средств защиты;
* использование программных средств для модификации средств защиты, позволяющих осуществить НСД;
* внедрение в АС вредоносных программ для осуществления НСД к информации или ее копирования.

**Разновидности угроз на сетевом уровне:**

а) скрытый отказ в обслуживании, вызванный привлечением части ресурсов автоматизированной системы (АС) на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов;

б) явный отказ в обслуживании, вызванный исчерпанием ресурсов АС при обработке пакетов, передаваемых злоумышленником;

в) явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами АС при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных;

г) явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «Nuke», «UDP-bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

**14.Способы непосредственного НСД к информации с использованием программных средств. Способы удаленного НСД к информации с использованием программных средств.**

**Способы непосредственного доступа**

**Первая группа** включает в себя способы, реализуемые в ходе загрузки операционной системы. Эти способы направлены на перехват паролей или идентификаторов, модификацию программного обеспечения базовой системы ввода/вывода (BIOS), перехват управления загрузкой с изменением необходимой технологической информации для получения несанкционированного доступа в операционную среду АС. Чаще всего такие способы реализуются с использованием отчуждаемых носителей информации.

**Вторая группа** – способы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем. Эти способы, как правило, направлены на выполнение непосредственно НСД к информации.

**Третья группа** включает в себя способы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. В большинстве случаев реализация этих способов связана с внедрением вредоносных программ.

**Основными видами вредоносных программ,** обеспечивающих НСД к информации, являются:

* программные кейлоггеры (клавиатурные шпионы);
* программы подбора и вскрытия паролей (программы-взломщики паралей);
* программы для скрытого наблюдения за компьютером (типа Actual Spy);
* программы для скрытного удаленного управления и администрирования (троянские программы типа Back Orifice, Backdoor, штатные средства управления и администрирования компьютерных сетей типа Landesk Management Suite, Managewise и т.п.);
* программы для несанкционированного скрытого копирования файлов (типа USBDumper) и т.д.

**Способы удаленного доступа**

* **анализ сетевого трафика** (способ реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль);
* **сканирование сети** (сущность способа заключается в передаче запросов сетевым службам хостов АС и анализе ответов от них с целью выявления используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определения активных сетевых сервисов, подбора идентификаторов и паролей пользователей);
* **выявление пароля** (суть способа состоит в использовании специальных программ выявления паролей, основанных на различных методах (например, простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля (например, программы «password sniffer», позволяющей выделять пользовательские идентификаторы и пароли из сетевого трафика при работе протоколов высокого уровня (ftp, telnet, rlogin и т.д.);
* **подмена доверенного объекта сети** и передача по каналам связи сообщений от его имени с присвоением его прав доступа (под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу;
* **навязывание ложного маршрута сети** (способ реализуется путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации. Реализация способа основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений   
  в маршрутно-адресные таблицы);
* **внедрение ложного объекта сети** (способ основан на использовании недостатков алгоритмов удаленного поиска);
* **удаленный запуск приложений** (способ заключается в стремлении запустить на хосте АС различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы» и т.д. )

**15. Несанкционированное воздействие на информацию. Классификация способов несанкционированного воздействия на информацию. Программно-математическое воздействие на информацию. Вредоносные программы.**

**Классификация способов несанкционированного воздействия на информацию**

К **угрозам целостности информации** относятся угрозы модифицирования (искажения, подмены) информации и угрозы уничтожения или повреждения информации, а к **угрозам доступности** − угрозы блокирования доступа к информации (cоздание условий, препятствующих доступу к информации субъекту, имеющему право на него).

**Нарушение целостности информации** осуществляется за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию.

**Нарушение доступности информации** обеспечивается путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

В вычислительных сетях нарушение доступности информации часто называют **отказом в обслуживании**, так как в результате этой угрозы операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Источником угрозы (непосредственной причиной возникновения угрозы) безопасности информации могут быть как физическое лицо, материальный объект, так и процесс или физическое явление.

Причины **непреднамеренного несанкционированного воздействия на информацию**:

* природные явления, стихийные бедствия (пожары, наводнения, землетрясения, грозовые разряды и т.д.);
* непреднамеренные электромагнитное или радиоционное облучение технических средств обработки информации (ТСОИ) и носителей информации;
* дефекты, сбои, отказы, аварии ТСОИ;
* дефекты, сбои и отказы программного обеспечения ТСОИ;
* дефекты, сбои, отказы, аварии систем и средств обеспечения ТСОИ;
* ошибки обслуживающего персонала объекта информатизации (ошибки при эксплуатации ТСОИ и программных средств ТСОИ, ошибки при эксплуатации средств и систем защиты информации) и т.д.

**Преднамеренные угрозы целостности и доступности информации**:

* использование специальных программных (программнно-математических) воздействий на информацию и программное обеспечение ТСОИ;
* использование специальных программно-технических воздействий на информацию, ТСОИ и программное обеспечение;
* преднамеренное силовое электромагнитное воздействие на информацию, ТСОИ и носители информации;
* диверсии в отношении объекта информатизации и т.д.

**Под программным (программно-математическим) воздействием** понимается несанкционированное воздействие, осуществляемое с использованием вредоносных программ (программ с потенциально опасными последствиями).

**Вредоносной программой** называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

* скрывать признаки своего присутствия в программной среде компьютера;
* обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
* разрушать (искажать произвольным образом) код программ в оперативной памяти;
* выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирование, уничтожение, блокирование и т.п.);
* сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
* искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Основными **видами вредоносных п**рограмм являются :

* программные закладки;
* классические программные (компьютерные) вирусы;
* вредоносные программы, распространяющиеся по сети (сетевые черви).

К **программным закладкам** относятся программы, фрагменты кода, инструкции, формирующие недекларированные возможности программного обеспечения.

**16.Классификация нарушителей НСД к информации.**

По наличию права доступа в контролируемую зону (КЗ) объекта информатизации и к АС **нарушители** подразделяются на два типа:

1. нарушители, не имеющие физического доступа к АС (внешние нарушители);
2. нарушители, имеющие физический доступ к АС (внутренние нарушители).

**Внешний нарушитель** может осуществлять НСД только к АС, подключенным к сетям связи общего пользования и (или) сетям международного информационного обмена.

Внешними нарушителями могут быть:

* разведывательные службы иностранных государств;
* криминальные структуры;
* конкуренты (конкурирующие организации);
* недобросовестные партнеры;
* внешние субъекты (физические лица).

**Внутренние нарушители (уровни):**

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС − запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

**Внутренние нарушители (категории)**

К первой категорииотносятся лица, имеющие санкционированный доступ к АС, но не имеющие доступа к защищаемой информации ограниченного доступа (далее - защищаемой информации).

Ко второй категорииотносятся зарегистрированные пользователи АС, осуществляющие доступ к защищаемой информации с рабочего места и имеющие ограниченные права доступа к ресурсам АС;

К третьей категорииотносятся зарегистрированные пользователи АС, осуществляющие удаленный доступ к защищаемой информации по локальным и (или) распределенным информационным системам.

К четвертой категорииотносятся зарегистрированные пользователи АС с полномочиями администратора безопасности сегмента (фрагмента) АС.

К пятой категорииотносятся зарегистрированные пользователи с полномочиями системного администратора АС.

К шестой категорииотносятся зарегистрированные пользователи с полномочиями администратора безопасности АС.

К седьмой категорииотносятся программисты-разработчики (поставщики) прикладного программного обеспечения и лица, обеспечивающие его сопровождение на объекте информатизации.

К восьмой категории относятся разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АС на объекте информатизации.

**17. Классификация и характеристика способов (методов) защиты информации от НСД.**

**Способы (методы) и защиты информации от НСД:**

* ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку информации, а также хранятся носители информации;
* реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам (идентификация и аутентификация );

**Способы идентификации и аутентификации пользователей:**

* с использованием простого пароля;
* в диалоговом режиме с использованием нескольких паролей и/или персональной информации пользователей;
* по биометрическим характеристикам человека (отпечатки пальцев, геометрия руки, голос, персональная роспись, структура сетчатки глаза, фотография и т.д.);
* по специальным устройствам (жетонам, картам, электронным ключам, радиокодовым устройствам и т.д.).
* разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

**Способы разграничения доступа:**

1. по уровням (кольцам) секретности (мандатное управление доступом)

* защищаемые данные распределяются по массивам (базам) таким образом, чтобы в каждом массиве (каждой базе) содержались данные одного уровня секретности;
* пользователю разрешается доступ к массиву (базе) своего уровня и массивам (базам) низших уровней, и запрещается доступ к массивам (базам) более высоких уровней

1. по специальным спискам (дискреционное управление доступом)

* для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу,
* или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа

1. по так называемым матрицам полномочий (дискреционное управление доступом)
2. по специальным мандатам (мандатное управление доступом)

* регистрация действий пользователей и обслуживающего персонала, контроль НСД и действий пользователей, обслуживающего персонала и посторонних лиц;
* учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
* резервирование технических средств, дублирование массивов и носителей информации;
* использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (сертификация СЗИ);
* предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок (антивирусная защита).
* использование защищенных каналов связи (криптографическая защита информации);
* размещение технических средств, позволяющих осуществлять обработку информации, в пределах охраняемой территории;
* организация физической защиты помещений и технических средств, позволяющих осуществлять обработку информации;

(при взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) :

* межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
* обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности информации;
* анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
* защита информации при ее передаче по каналам связи (криптографическая защита информации);
* использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
* использование средств антивирусной защиты;
* централизованное управление системой защиты информации информационной системы.

**18.Сертифицированные программные средства защиты информации от НСД.**

В настоящее время среди основных игроков рынка сертифицированных СЗИ от НСД можно выделить:

* СЗИ от НСД Secret Net, Secret Net Studio и ПАК «Соболь» («Код Безопасности»)
* СЗИ от НСД Dallas Lock (компания «Конфидент»)
* СЗИ от НСД «Аккорд» (компания ОКБ САПР)
* СЗИ от НСД «Блокхост-сеть К» и «Блокхост-АМДЗ 2.0» («Газинформсервис»)
* СЗИ от НСД ПАНЦИРЬ (НПП «Безопасные информационные технологии»)
* СЗИ от НСД Diamond ACS (компания ТСС)
* СЗИ от НСД «Страж NT 4.0» (компания «Рубинтех»)
* СЗИ от НСД «Аура» (СПИИРАН) СЗИ от НСД «Фантом» (РНТ)

**СЗИ Secret Net предназначено для решения следующих типовых задач:**

* Защита информации на рабочих станциях и серверах в соответствии с требованиями регулирующих органов
* Контроль утечек и каналов распространения защищаемой информации

**Основные возможности:**

* Разграничение доступа
* Контроль утечек
* Защита VDI-инфраструктуры
* Централизованное управление
* Система отчетов
* Высокая масштабируемость

Имеет сертификаты соответствия ФСТЭК России и Мин. обороны РФ.

Производитель [ООО «Код Безопасности»](http://www.securitycode.ru/)

**СЗИ Dallas Lock 8.0-K** представляет собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

Обеспечивает:

* защиту информации от несанкционированного доступа;
* поддержку виртуальных сред;
* дискреционный принцип разграничения доступа к информационным ресурсам и подключаемым устройствам в соответствии с матрицей доступа;
* аудит действий пользователей;
* контроль целостности файловой системы, программно-аппаратной среды и реестра;
* объединение защищенных ПЭВМ для централизованного управления механизмами безопасности;
* приведение АС, ГИС, АСУ ТП и систем обработки персональных данных в соответствие законодательству РФ по защите информации.

Имеет сертификат соответствия ФСТЭК России № 2720 от 25.09.2012.

Производитель [ЦЗИ «Конфидент»](https://www.dallaslock.ru/).

**Электронный замок «Соболь» предназначен для решения следующих типовых задач:**

* Защита компьютеров от несанкционированного доступа и обеспечение доверенной загрузки
* Создание доверенной программной среды для повышения класса защиты СКЗИ

**Основные возможности МДЗ «Соболь»:**

* Идентификация и аутентификация
* Контроль целостности
* Аппаратный ДСЧ
* Регистрация попыток доступа
* Доверенная загрузка
* Сторожевой таймер

Имеет сертификаты соответствия ФСТЭК России и ФСБ в России.

Производитель [ООО «Код Безопасности»](http://www.securitycode.ru/)

**19.Сертифицированные САВЗ. Методы обнаружения вирусов.**

**Сертифицированные средства антивирусной защиты:**

* Антивирус для рабочих станций Avast Avast Free Antivirus
* Аутентификация Алладин Р.Д. JaCarta Management System
* Антивирус для рабочих станций Лаборатория Касперского Kaspersky Endpoint Security
* Защита баз данных МФИ Софт Гарда БД
* Антивирус для файловых серверов Лаборатория Касперского Kaspersky Security 10 для Windows Servers
* Защита виртуальных сред Конфидент Dallas Lock
* Комплексная защита конечных точек Доктор Веб Dr.Web Enterprise Security Suite
* Аутентификация Алладин Р.Д. eToken
* ESET NOD32 Secure Enterprise Pack 5.0
* Межсетевой экран Cisco ASA 5525

**Методики обнаружения и защиты от вирусов**

* + сканирование
* Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов
* Под сигнатурой понимается уникальная последовательность байт, принадлежащая вирусу, и не встречающаяся в коде других программах.
  + эвристический анализ
* Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе, как этого требует, например, метод обнаружения изменений.
* Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов.
* Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы.
  + использование антивирусных мониторов
* Существует целый класс антивирусных программ, которые постоянно находятся в памяти компьютера, и отслеживают все подозрительные действия, выполняемые другими программами
* Такие программы носят название антивирусных мониторов или сторожей.
* Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты и компакт диска.
* Антивирусный монитор сообщает пользователю, в случае ситуации, когда какая-либо программа попытается выполнить потенциально опасное действие.
  + обнаружение изменений
* Когда вирус заражает компьютер, он изменяет содержимое жесткого диска, например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса, изменяет загрузочный сектор, создает файл-спутник.
* Таких изменений, однако, не делают «бестелесные» вирусы, обитающие не на диске, а в памяти процессов ОС.
* Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам.
* Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название программы-ревизоры).
  + использование антивирусов, встроенных в BIOS компьютера
* В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов
* Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет
* Если какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов.

**20.Сертифицированные программно-аппаратные средства защиты информации от НСД.**

По типу исполнения СЗИ от НСД бывают программными и программно-аппаратными. К последним относятся комплексы, где помимо специального программного обеспечения для разграничения доступа к ресурсам в составе комплекса есть аппаратный модуль — средство доверенной загрузки.

**ПАК «Блокхост-МДЗ»**

Программно-аппаратный комплекс «Блокхост-МДЗ» предназначен для решения следующих задач: двухфакторная аутентификация пользователей для усиления защиты входа на рабочую станцию до загрузки операционной системы; обеспечение конфиденциальности данных, хранимых на электронных носителях, путем шифрования их содержимого; контроль целостности файлов с заданной периодичностью; выполнение гарантированного удаления файлов без возможности их восстановления; очистка областей оперативной памяти после завершения контролируемых процессов для предотвращения считывания остаточной информации; сохранение конфиденциальности данных даже при краже или утере носителей; контроль доступа пользователей к отчуждаемым носителям, оптическим приводам, Wi-Fi и Bluetooth-адаптерам, подключаемым через USB порты. «Блокхост-МДЗ» состоит из 7 модулей, которые могут быть использованы как единым комплексом, так и по отдельности.

Продуктовая линейка **«Аккорд» компании ОКБ САПР** представлена программно-аппаратными комплексами для защиты Windows и Linux рабочих мест и серверов, которая включает:

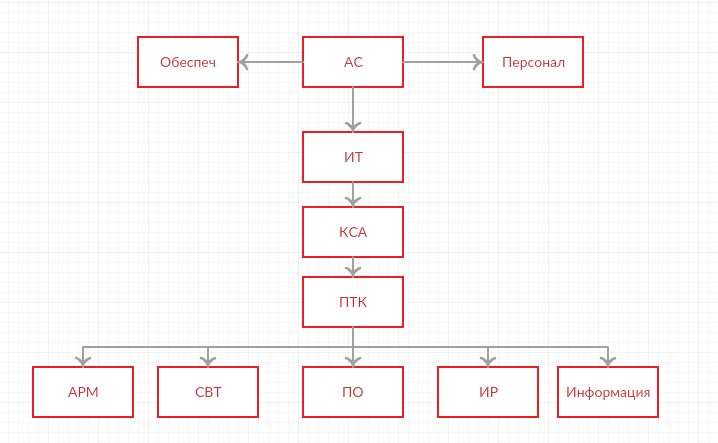
* «Аккорд-АМДЗ» — аппаратный модуль доверенной загрузки.
* Программно-аппаратные комплексы «Аккорд-Win32», «Аккорд-Win64» — для разграничения доступа пользователей к рабочим станциям и серверам, работающим под управлением 32- и 64-разрядных Windows.
* Программно-аппаратные комплексы Аккорд-Х, Аккорд-Х К — для разграничения доступа пользователей к рабочим станциям и серверам под управлением Linux.
* СУЦУ — система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд».

Компания ТСС для защиты автоматизированных рабочих мест и серверов предлагает программно-аппаратный комплекс **Diamond ACS.**

Это кроссплатформенный программно-аппаратный комплекс средств защиты информации от несанкционированного доступа. Продукт позволяет осуществлять доверенную загрузку и физическое разделение контуров различной степени конфиденциальности на автоматизированных рабочих местах.

**21.Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС.**

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.



КСА – комплекс средств автоматизации

ПТК (программно-технический комплекс) - Продукция, представляющая собой совокупность СВТ, ПО и ИР, достаточных для выполнения одной или более задач АС.

АРМ (Автоматизированное рабочее место) - Программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида

ПО (Программное обеспечение) - программа или множество программ, используемых для управления компьютером.

**Классы защищенности АС от НСД к информации**

**Третья группа** классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

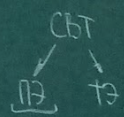
**Вторая группа** классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

**Первая группа** классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **ГосТайна** | | | **Конфиден. Информация** | |  |
|  | **С** | | | **ПДн** | |  |
| **СС** | |  |
| **ОВ** |  |  | **СлужТайна** |  |
| **I** | **1А** | **1Б** | **1В** | **1Г** | **1Д** | **многопользовательская с разными правами** |
| **II** | **2А** |  |  | **2Б** |  | **многопользовательская с одинаковыми правами** |
| **III** | **3А** |  |  | **3Б** |  | **однопользовательская** |

**22.Средства вычислительной техники. Защита от несанкционированного доступа к информации. Классификация СВТ.**

**Средства вычислительной техники** – совокупность программных и технических элементов, предназначенных для обработки данных, способных функционировать самостоятельно или в составе систем.



Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс – седьмой, самый высокий – первый. Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

1. содержит только один седьмой класс;
2. **дискреционная** защита и содержит шестой и пятый классы;
3. **мандатная** защита и содержит четвертый, третий и второй классы;
4. **верифицированная** защита и содержит только первый класс.

**23. Основные требования к подсистеме регистрации и учета АС.**

**Подсистема регистрации и учета** должна:

1. Регистрировать вход (выход) субъектов доступа в систему (из системы), либо регистрировать загрузку и инициализацию операционной системы. При этом в параметрах регистрации указываются:

• дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

• результат попытки входа — успешная или неуспешная (при НСД);

• идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

• код или пароль, предъявленный при неуспешной попытке.

Регистрация выхода из системы или остановка не проводится в моменты аппаратурного отключения АС.

2. Регистрировать выдачу печатных (графических) документов на твердую копию. При этом в параметрах регистрации указываются:

• дата и время выдачи (обращения к подсистеме вывода);

• краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности;

• спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

• идентификатор субъекта доступа, запросившего документ.

3. Регистрировать запуск (завершение) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов.

При этом в параметрах регистрации указывается:

• дата и время запуска;

• имя (идентификатор) программы (процесса, задания);

• идентификатор субъекта доступа, запросившего программу (процесс, задание);

• результат запуска (успешный, неуспешный — несанкционированный).

4. Регистрировать попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указывается:

• дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная — несанкционированная);

• идентификатор субъекта доступа;

• спецификация защищаемого файла.

5. Регистрировать попытки доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. При этом в параметрах регистрации указывается:

• дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная, несанкционированная;

• идентификатор субъекта доступа;

• спецификация защищаемого объекта [логическое имя (номер)].

6. Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

7. Регистрировать выдачу (приемку) защищаемых носителей.

8. Осуществлять очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. При этом очистка должна производиться однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

**24.Основные требования к подсистеме обеспечения целостности АС.**

**Подсистема обеспечения целостности**должна:

1. Обеспечивать целостность программных средств системы защиты информации от НСД (СЗИ НСД), обрабатываемой информации, а также неизменность программной среды. При этом:

• целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;

• целостность программной среды обеспечивается использованием трансляторов с языка высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

2. Осуществлять физическую охрану СВТ (устройств и носителей информации). При этом должны предусматриваться контроль доступа в помещение АС посторонних лиц, а также наличие надежных препятствий для несанкционированного проникновения в помещение АС и хранилище носителей информации. Особенно в нерабочее время.

3. Проводить периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест программ, имитирующих попытки НСД.

4. Иметь в наличии средства восстановления СЗИ НСД. При этом предусматривается ведение двух копий программных средств СЗИ НСД, а также их периодическое обновление и контроль работоспособности.

**25.Основные требования к подсистеме управления доступом АС.**

**Подсистема управления доступом**должна удовлетворять следующим требованиям:

1. Идентифицировать и проверять подлинность субъектов доступа при входе в систему. Причем это должно осуществляться по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

2. Идентифицировать терминалы, ЭВМ, узлы компьютерной сети, каналы связи, внешние устройства ЭВМ по их логическим адресам (номерам).

3. По именам идентифицировать программы, тома, каталоги, файлы, записи и поля записей.

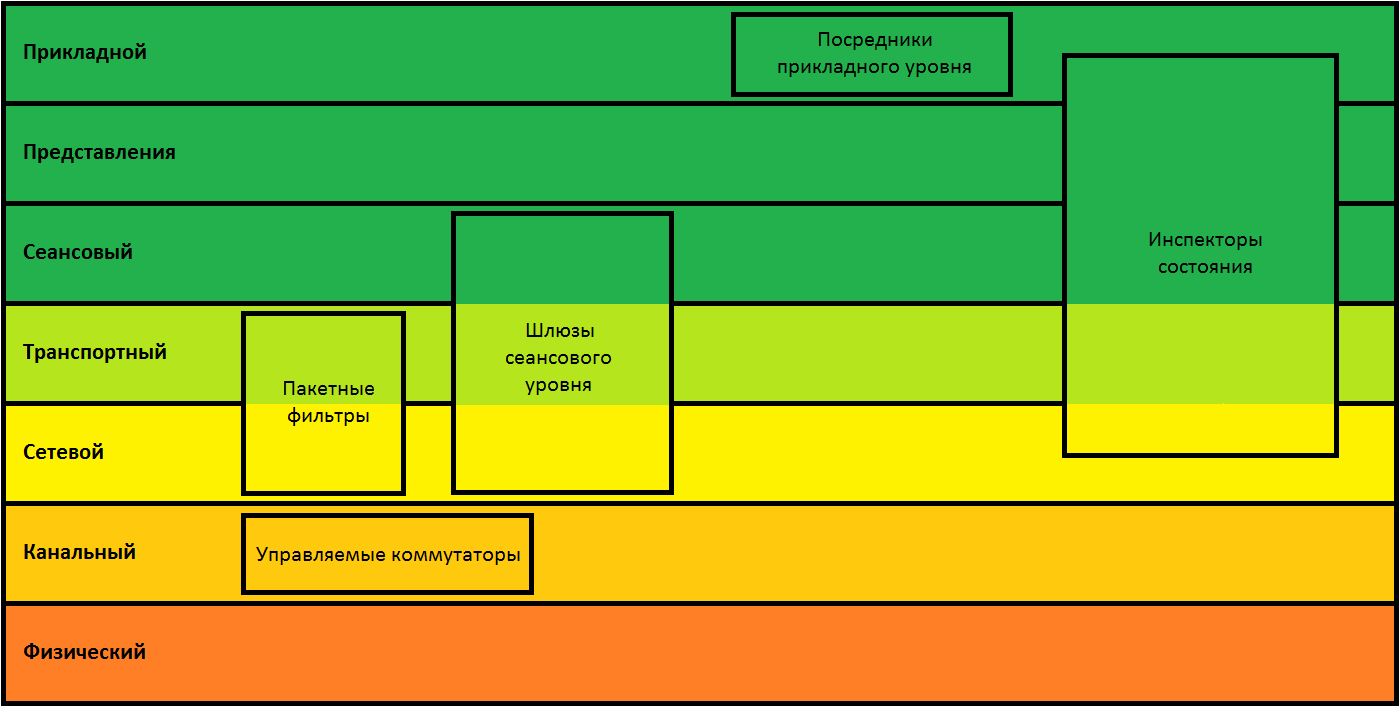
4. Осуществлять контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа

**26. Межсетевые экраны (определение). Классификация. Классы защищенности МЭ.**

**Межсетевой экран** - локальный (однокомпонентный) или функционально-распределенный программный или программно-аппаратный элемент (комплекс), реализующий контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Учитывая модель OSI, различают следующие типы межсетевых экранов:

1. Управляемые коммутаторы.
2. Пакетные фильтры.
3. Шлюзы сеансового уровня.
4. Посредники прикладного уровня.
5. Инспекторы состояния.



Устанавливается пять классов защищенности МЭ.

* Пятый - самый низкий класс защищенности, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой;
* четвертый - для 1Г;
* третий - 1В;
* второй - 1Б;
* первый 1А.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

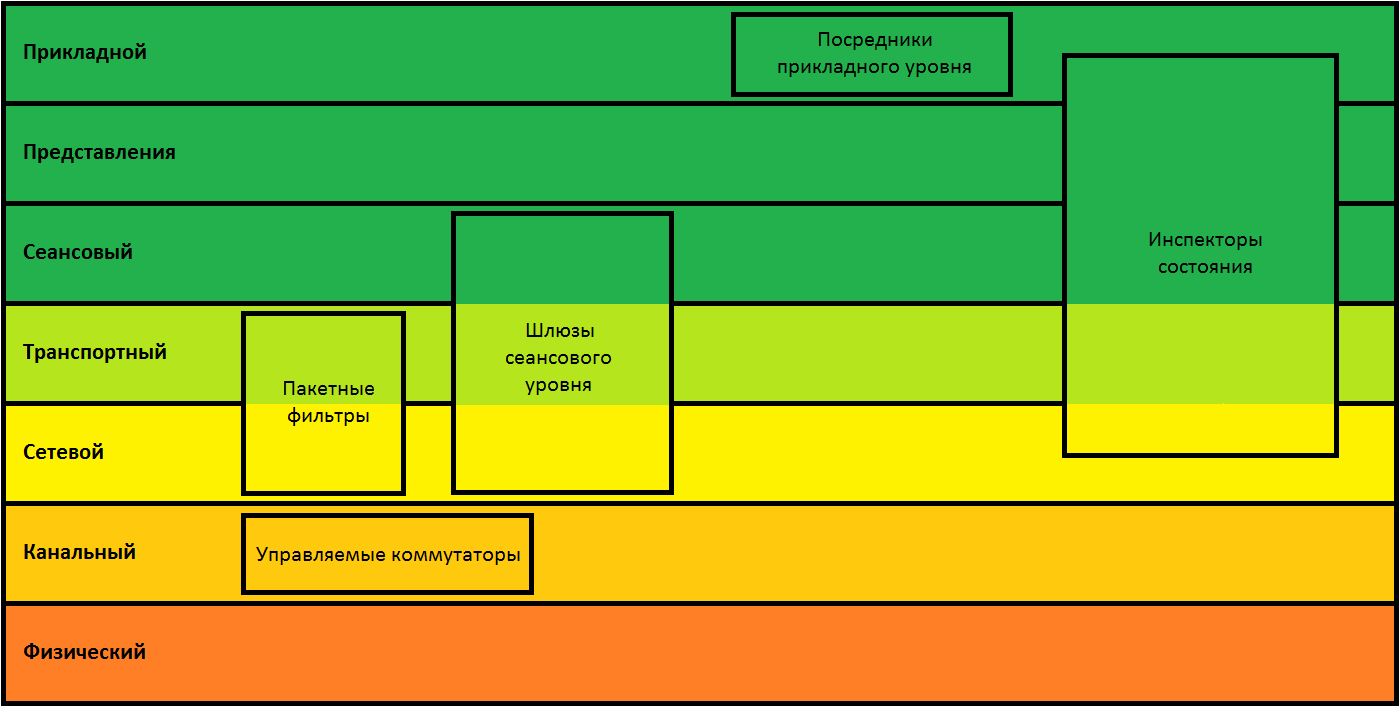
* при обработке информации с грифом “секретно” - не ниже 3 класса;
* при обработке информации с грифом “совершенно секретно” - не ниже 2 класса;
* при обработке информации с грифом “особой важности” - не ниже 1 класса.

**27. Межсетевые экраны (определение). Классификация. Показатели защищенности МЭ.**

**Межсетевой экран** - локальный (однокомпонентный) или функционально-распределенный программный или программно-аппаратный элемент (комплекс), реализующий контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Учитывая модель OSI, различают следующие типы межсетевых экранов:

1. Управляемые коммутаторы.
2. Пакетные фильтры.
3. Шлюзы сеансового уровня.
4. Посредники прикладного уровня.
5. Инспекторы состояния.



**Показатели защищенности** применяются к МЭ для определения уровня защищенности, который они обеспечивают.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Показатели защищенности | Классы защищенности | | | | |
| 5 | 4 | 3 | 2 | 1 |
| Управление доступом (фильтрация данных и трансляция адресов) | + | + | + | + | = |
| Идентификация и аутентификация | - | - | + | = | + |
| Регистрация | - | + | + | + | = |
| Администрирование: идентификация и аутентификация | + | = | + | + | + |
| Администрирование: регистрация | + | + | + | = | = |
| Администрирование: простота использования | - | - | + | = | + |
| Целостность | + | = | + | + | + |
| Восстановление | + | = | = | + | + |
| Тестирование | + | + | + | + | + |
| Руководство администратора защиты | + | = | = | = | = |
| Тестовая документация | + | + | + | + | + |
| Конструкторская (проектная) документация | + | = | + | = | + |

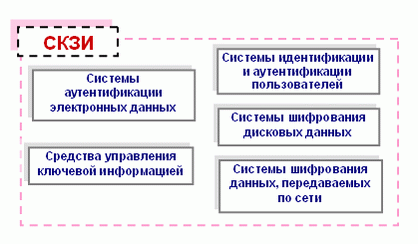
- Требований нет;   
= Требования такие же, как и у класса уровнем ниже;   
+ Требования дополняются по сравнению с классом уровнем ниже.

**28. Криптографическая защита информации. Классификация криптографических средств. Основные методы шифрования.**

**Криптографическая защита информации** - защита информации с помощью ее криптографического преобразования.

**К средствам криптографической защиты информации** (СКЗИ), относятся аппаратные, программно-аппаратные и программные средства, реализующие криптографические алгоритмы преобразования информации.

**Шифратор** - аппарат или программа, реализующая алгоритм шифрования. Введенное понятие СКЗИ включает в себя шифратор, но в целом является более широким.



1. **Системы идентификации и аутентификации пользователей.** Такие системы применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы этих систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

2. **Системы шифрования дисковых данных.** Основная задача, решаемая такими системами, состоит в защите от несанкционированного использования данных, расположенных на дисковых носителях.

Системы шифрования данных могут осуществлять криптографические преобразования данных:

* на уровне файлов (защищаются отдельные файлы);
* на уровне дисков (защищаются диски целиком).

К программам первого типа можно отнести архиваторы типа WinRAR, которые позволяют использовать криптографические методы для защиты архивных файлов.

Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities.

По способу функционирования системы шифрования дисковых данных делят на два класса:

1. системы “прозрачного” шифрования;
2. системы, специально вызываемые для осуществления шифрования.

В системах *прозрачного шифрования* (шифрования “на лету”) криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

3. **Системы шифрования данных, передаваемых по компьютерным сетям.**

Различают два основных способа шифрования:

1. канальное шифрование;
2. оконечное (абонентское) шифрование.

В случае канального шифрования защищается вся передаваемая по каналу связи информация, включая служебную. Соответствующие процедуры шифрования реализуются с помощью протокола канального уровня семиуровневой эталонной модели взаимодействия открытых систем OSI (Open System Interconnection).

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя прикладными объектами (абонентами). Оконечное шифрование реализуется с помощью протокола прикладного или представительного уровня эталонной модели OSI. В этом случае защищенным оказывается только содержание сообщения, вся служебная информация остается открытой.

4. **Системы аутентификации электронных данных** (например, аутентификации автора документа и самого документа).

Для аутентификации электронных данных применяют код аутентификации сообщения (имитовставку) или электронную цифровую подпись.

Имитовставка - блок информации, вычисленный по определенному закону и зависящий от некоторого криптографического ключа и данных.

Электронная (цифровая) подпись - присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

При формировании кода аутентификации сообщения и электронной цифровой подписи используются разные типы систем шифрования.

5. **Средства управления ключевой информацией.**

Под ключевой информацией понимается совокупность всех используемых в компьютерной системе или сети криптографических ключей.

Различают следующие основные виды функций управления ключами:

1. генерация ключей;
2. хранение ключей;
3. распределение ключей.

Способы *генерации ключей* различаются для симметричных и асимметричных криптосистем.

Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел.

Генерация ключей для асимметричных криптосистем представляет существенно более сложную задачу в связи с необходимостью получения ключей с определенными математическими свойствами.

Функция *хранения ключей* предполагает организацию безопасного хранения, учета и удаления ключей. Для обеспечения безопасного хранения и передачи ключей применяют их шифрование с помощью других ключей.

*Концепция иерархии ключей*.

В иерархию ключей обычно входят главный ключ (мастер-ключ), ключ шифрования ключей и ключ шифрования данных.

Генерация и хранение мастер-ключей являются критическими вопросами криптографической защиты.

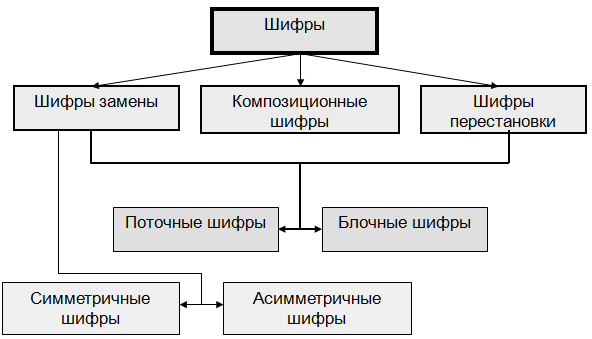
*Распределение ключей* является самым ответственным процессом в управлении ключами.

Различают два основных способа распределения ключей между пользователями компьютерной сети:

1. применение одного или нескольких центров распределения ключей;
2. прямой обмен сеансовыми ключами между пользователями.

**Шифрование** — это преобразование данных в вид, недоступный для чтения без ключа шифрования. **Методом шифрования** (шифром) называется совокупность обратимых преобразований открытой информации в закрытую информацию в соответствии с алгоритмом шифрования.

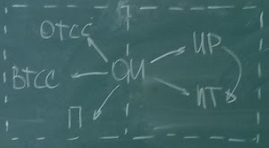
**Основные методы шифрования:**

****

* Методы замены или подстановки - символы исходного текста заменяются на символы другого (или того же) алфавита в соответствии с заранее определенной схемой, которая и будет ключом данного шифра.
* Симметричные криптосистемы - для шифрования и для расшифрования используется один и тот же ключ;
* Системы с открытым ключом (ассиметричные) - для шифрования и расшифровывания используются два ключа - открытый и закрытый (секретный), которые математически связаны друг с другом.
* Методы перестановки - символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом.
* Методы гаммирования - символы исходного текста складываются с символами некой случайной последовательности.
* Методы, основанные на сложных математических преобразованиях исходного текста по некоторой формуле.
* Эффективным средством повышения стойкости шифрования является *комбинированное использование* нескольких различных методов.

**29. Объект информатизации (определение). Основные технические средства и системы (ОТСС). Вспомогательные технические средства и системы (ВТСС). Посторонние проводники. Технический канал утечки информации (определение). Схема технического канала утечки информации.**

**Объект информатизации** – совокупность информационных ресурсов (содержащих сведения ограниченного доступа), информационных технологий, ОТСС, ВТСС, персонала и помещений (или объектов) в которых они установлены.



***Информационные ресурсы –*** *отдельные документы (массивы документов), содержащиеся в информационных системах (библиотеках, архивах, фондах и т.д.)*

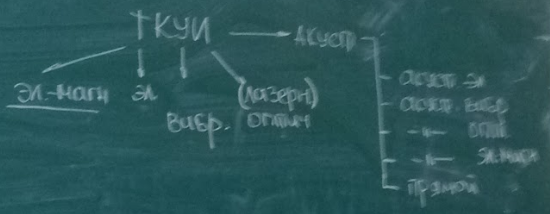
***Информационная технология*** *– приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации.*

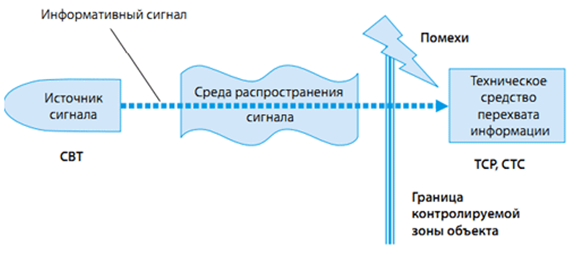
**Основные технические средства и системы** (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки информации ограниченного доступа.

**Вспомогательные технические средства и системы** (ВТСС) – технические средства и системы обеспечения объекта информатизации, непосредственно не участвующие в обработке информации ограниченного доступа.

**Посторонние проводники** (ПП) - провода и кабели, а также другие металлоконструкции, не относящиеся к ОТСС или ВТСС, но проходящие через помещения, где они установлены.

**ТКУИ**. **Технический канал утечки информации** – совокупность источника информативного сигнала, устройства приема сигнала и физической среды, в которой распространяется сигнал.

****

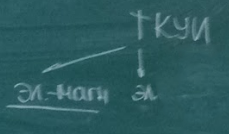


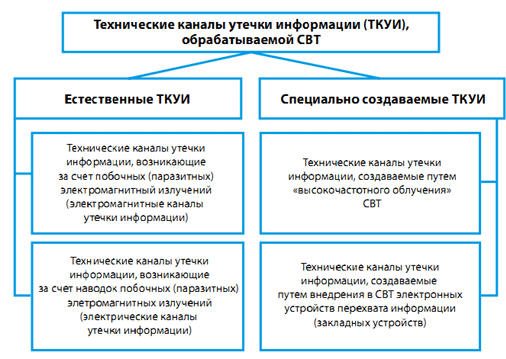
**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

**30.Классификация ТКУИ, обрабатываемых техническими СВТ.**

**СВТ - Средства вычислительной техники** – совокупность программных и технических элементов, предназначенных для обработки данных, способных функционировать самостоятельно или в составе систем.

**ТКУИ** - **Технические каналы утечки информации**. Совокупность источника информативного сигнала, устройства приема сигнала и физической среды, в которой распространяется сигнал.

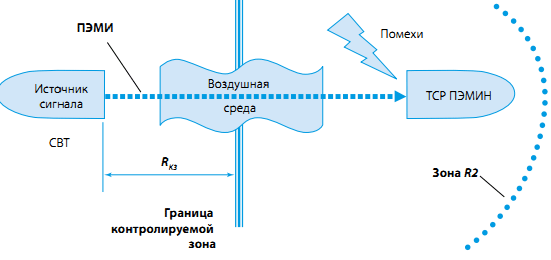






**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

**31.Схема ТКУИ, возникающего за счет побочных электромагнитных излучений. Определение зоны R2.**



**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

**ТКУИ** - **Технические каналы утечки информации**. Совокупность источника информативного сигнала, устройства приема сигнала и физической среды, в которой распространяется сигнал.

**Зона R2** – это зона, в пределах которой возможен перехват средством разведки ПЭМИ от ТСПИ с требуемым качеством. Опасная зона 2 (*R*2) – пространство вокруг СВТ, в пределах которого напряженность электрической и магнитной составляющей электромагнитного поля информативного сигнала превышает допустимое (нормированное) значение.

**ПЭМИ(Н)** - это Побочные ЭлектроМагнитные Излучения (и Наводки)

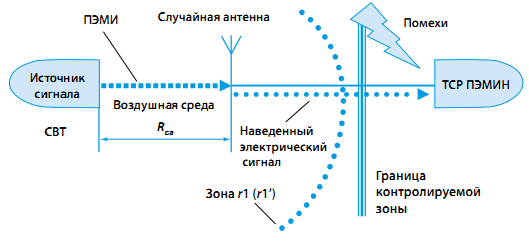
**32.Случайные антенны (определения). Схемы технических каналов утечки информации, возникающих за счет наводок побочных электромагнитных излучений. Определение зон r1 и r1’.**

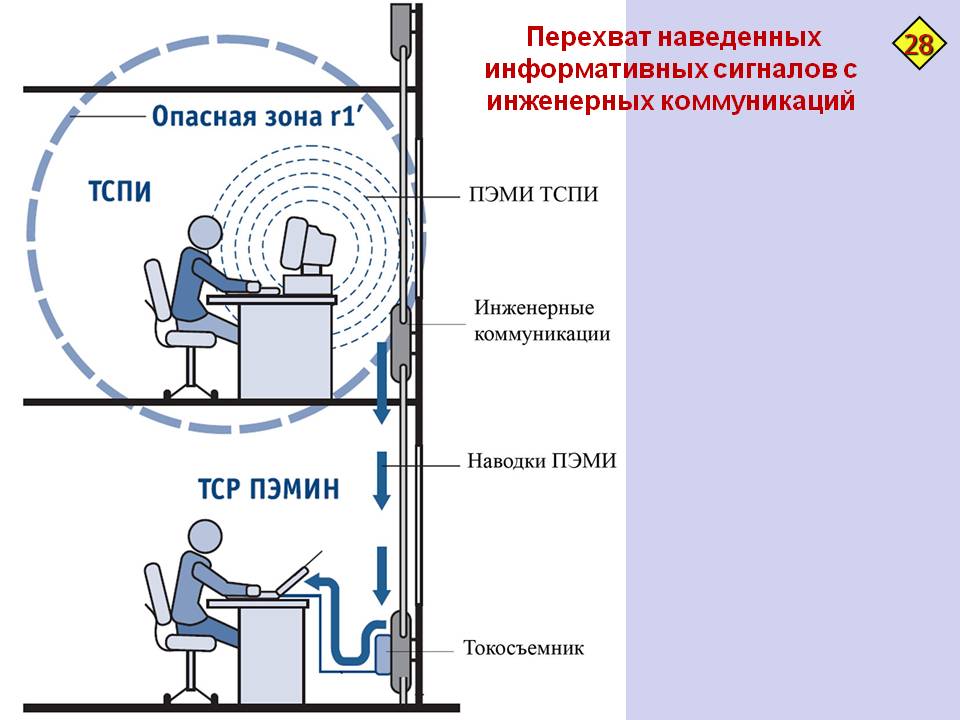
**Случайной антенной** являются ВТСС (Вспомогательные технические средства и системы) и их соединительные линии, а также посторонние проводники, способные принимать побочные электромагнитные излучения и выходящие за пределы контролируемой зоны. Они играют роль слу­чайных излучателей электромагнитных волн, при подключении к ко­торым возможен перехват информации.

К **сосредоточенным** случайным антеннам относятся различные компактные технические устройства и приспособления.

К **распределенным** случайным антеннам (РСА) относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

**ТКУИ** - **Технические каналы утечки информации**. Совокупность источника информативного сигнала, устройства приема сигнала и физической среды, в которой распространяется сигнал.





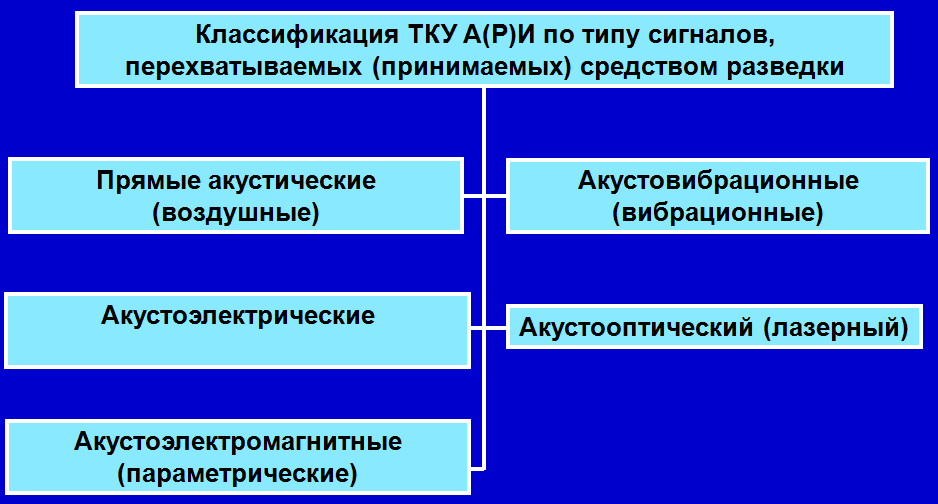
**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

Пространство вокруг ОТСС (Основные технические средства и системы), в пределах которого уровень наведенного от ОТСС информативного сигнала в сосредоточенных антеннах превышает допустимое значение, называется **зоной r1**, а в распределенных антеннах – **зоной r1’**.

**33.Выделенное помещение. Защищаемое помещение. Классификация технических каналов утечки акустической речевой информации.**

**Выделенное помещение -** помещение, специально предназначенное для проведения мероприятий, на которых происходит обработка информации **секретного** характера.

**Защищаемое помещение** – помещение, специально предназначенное для проведения мероприятий, на которых происходит обработка информации **конфиденциального** характера.



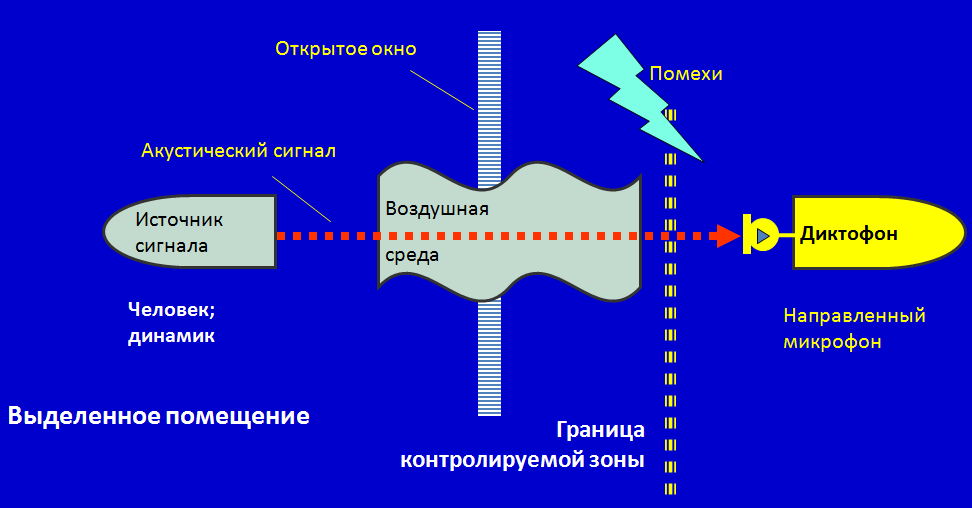
**34.Схемы прямых акустических каналов утечки акустической речевой информации. Направленные микрофоны, цифровые диктофоны, электронные устройства перехвата акустической речевой информации**

**Направленный микрофон** – это  микрофон, чувствительный к звуку в определенном направлении.

**Цифровой диктофон** — это устройство, с помощью которого можно произвести запись акустической информации на электронный носитель.

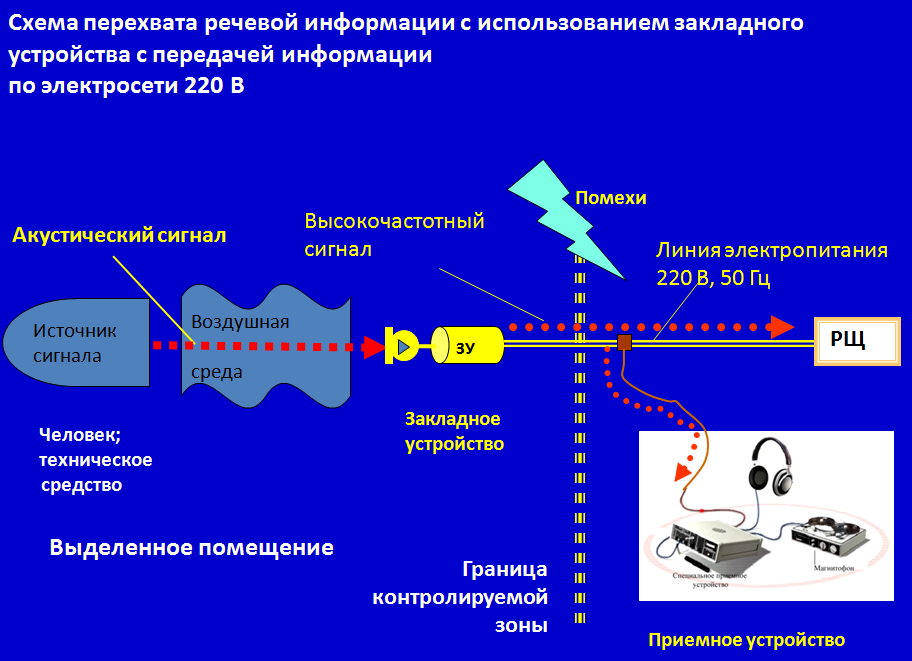
**Электронные устройства перехвата акустической речевой информации** - малогабаритные автономные автоматические средства акустической разведки, скрытно внедряемые в ВП или ЗП, или в смежные с ними помещения.

**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

**Схема перехвата речевой информации с использованием направленного микрофона  
**

**Схема перехвата речевой информации с использованием закладных устройств**

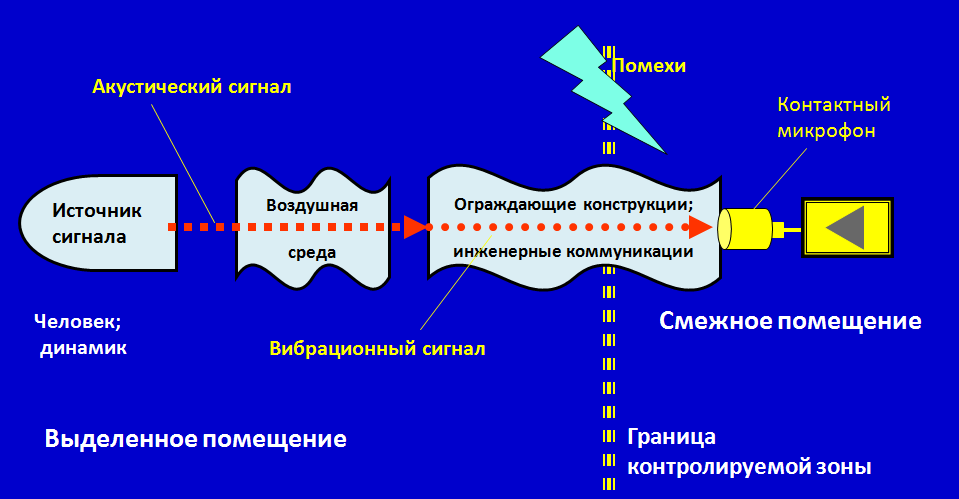








**35.Схемы акустовибрационных каналов утечки акустической речевой информации. Электронные стетоскопы, радиостетоскопы. Средства акустической разведки, осуществляющие перехват речевой информации по прямым акустическим каналам.**

****

**Средства акустической разведки, осуществляющие перехват речевой информации по акустовибрационным каналам** - устройства, регистрирующие вибрационные колебания, возникающие при воздействии на ограждающие конструкции и инженерные коммуникации акустических сигналов, возникающие при ведении разговоров.

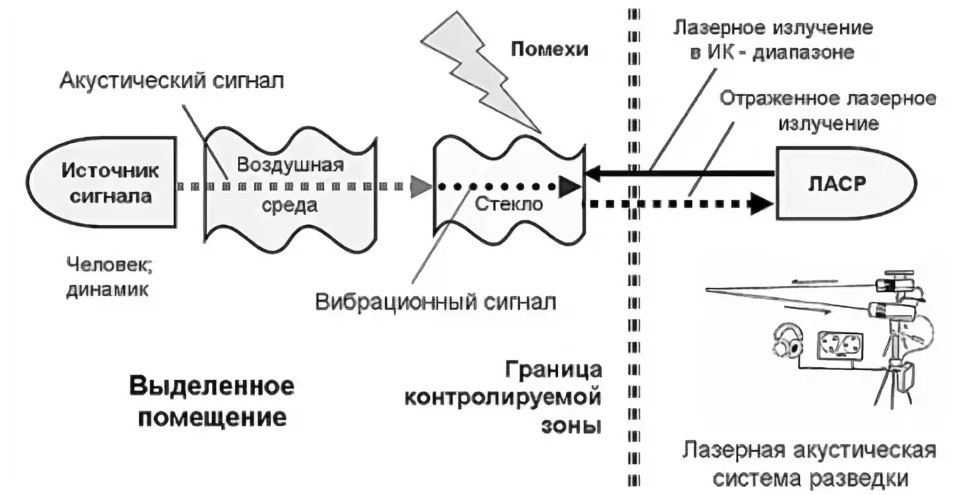
**Электронный стетоскоп –**устройство,регистрирующее вибрационные колебания в ограждающих конструкциях и инженерных коммуникациях, которое может записать или отправить перехваченную информацию в пункт приема информации. В электронных стетоскопах в качестве датчиков используются контактные микрофоны, которые преобразуют акустические колебания, распространяющиеся в твердых телах (стенах, потолках), в электрические.

**Радиостетоскоп -** электронный стетоскоп, использующий для передачи информации радиоканал.

**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

**Средства акустической разведки, осуществляющие перехват речевой информации по прямым акустическим каналам** – устройства, с помощью которых возможно произвести запись непосредственно акустической информации. К ним относятся направленный микрофон, диктофон, закладные устройства с датчиками микрофонного типа.

**36. Схема акустооптического канала утечки акустической речевой информации. Лазерные акустические системы разведки.**

****

**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

Перехват речевой информации путем «лазерного зондирования» оконных стекол

Луч лазера падает на оконное стекло, модулируется вибрационными сигналами стекла и отражается. Отраженный луч улавливается фотодетектором, и осуществляется демодуляция отраженного луча и запись или передача перехваченной информации.

Для упрощения зондирования используют триппель-призму – отражающий элемент, который обеспечивает возврат излучения в исходном направлении вне зависимости от угла падения на входе.

**37.Схемы акустоэлектрических и акустоэлектромагнитных каналов утечки акустической речевой информации.**

**Акустоэлектрические каналы утечки информации** – канал утечки, возникающий за счет микрофонного эффекта, например, на катушках индуктивности и звонках телефонных аппаратов появляется модуляция токов, в соответствии с изменениями воздействующих акустических сигналов, которые возможно перехватить, подключившись к линиям ВТСС или телефонной линии.

**Микрофонный эффект** — нежелательное явление, при котором некоторая часть электрической цепи воспринимает звуковые колебания и вибрацию подобно микрофону.

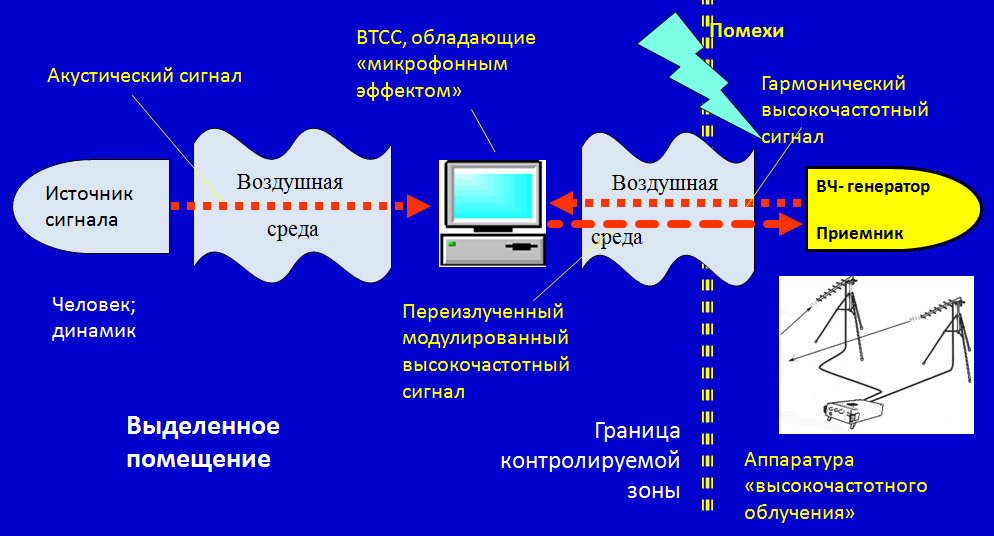
****

****

**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

**Акустоэлектромагнитный канал утечки информации** – канал утечки, возникающий за счет изменения давления на элементы высокочастотных генераторов ТСПИ и ВТСС. В них появляется модуляция токов, в соответствии с изменениями воздействующих акустических сигналов, которые излучаются в пространство в виде ПЭМИ. Также при помощи высокочастотного облучения возможно заставить переизлучать модулированный сигнал.

**Схема акустоэлектромагнитного(пассивного) канала утечки речевой информации**  

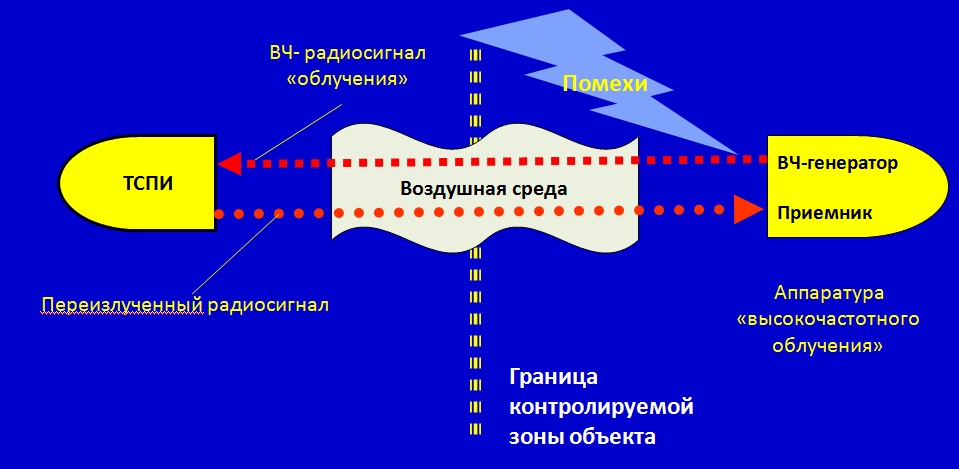

**Схема акустоэлектромагнитного (активного) канала утечки речевой информации**  
  


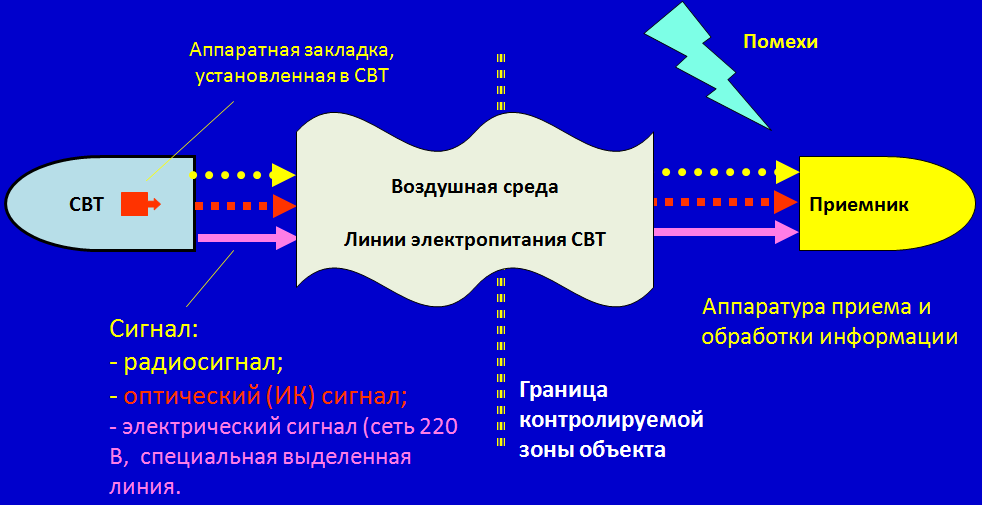
**38.Специально создаваемые каналы утечки информации, обрабатываемой СВТ. Аппаратные закладки.**

**Контролируемая зона (КЗ)** – это пространство, в котором исключено неконтролируемое пребывание посторонних лиц или посторонних транспортных средств.

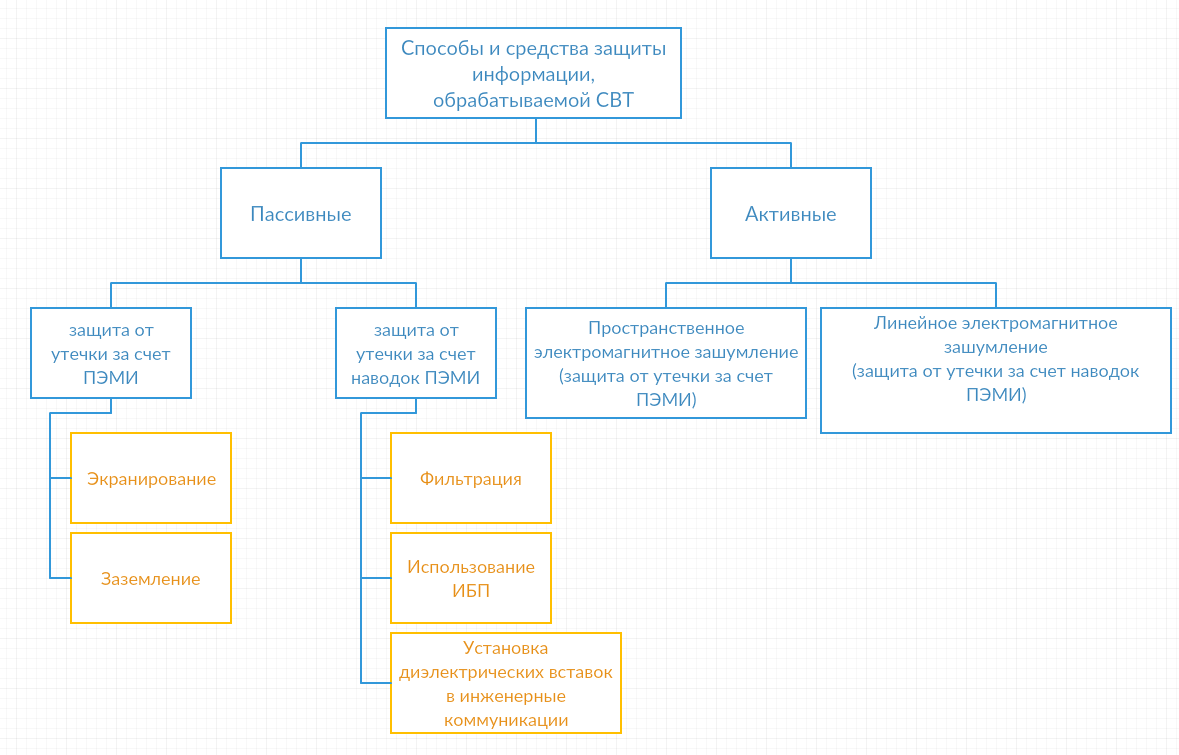
**Специально создаваемые** **ТКУИ** делятся на:

* Технические каналы утечки информации, создаваемые путем «высокочастотного облучения» ТСПИ

****

* Технические каналы утечки информации, создаваемые путем внедрения в ТСПИ электронных устройств перехвата информации (закладных устройств) ****

**Аппаратная закладка** (кейлоггер) предназначена для перехвата данных, вводимых с клавиатуры. Для активации закладки необходимо ее облучение гармоническим радиосигналом от специального генератора.

**39.Классификация способов и средств защиты информации, обрабатываемой СВТ, от утечки по техническим каналам.**

**ИБП** – источники бесперебойного питания.

**Экранирование**

* Локальное экранирование отдельных излучающих элементов (узлов) ТСПИ.
* Экранирование отдельных блоков ТСПИ.
* Экранирование соединительных линий и целей электропитания ТСПИ.
* Размещение ТСПИ в экранированном помещении (камере).

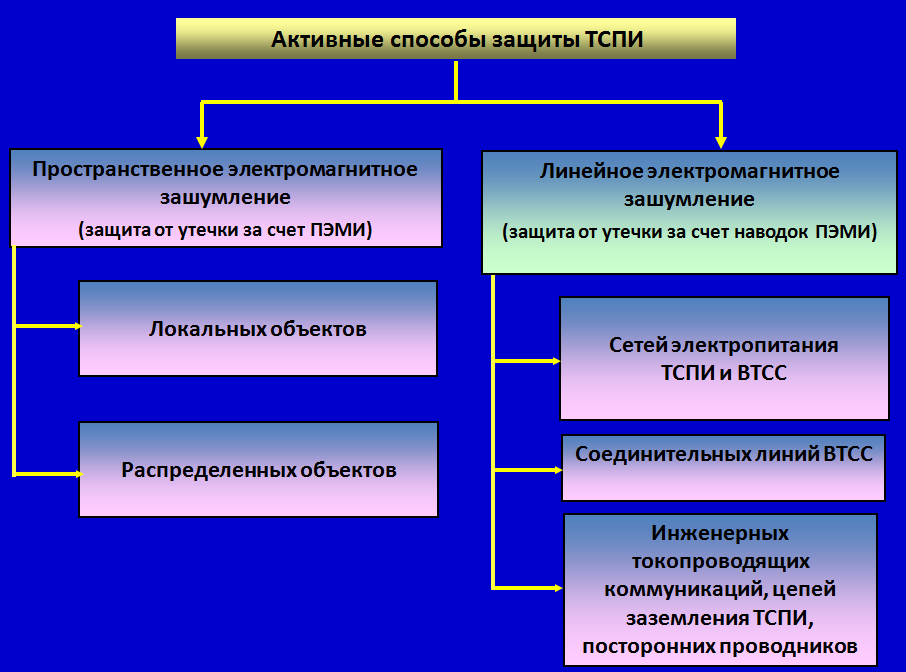
**Заземление**

* Заземление экранов элементов (узлов, блоков) ТСПИ.
* Заземление экранов соединительных линий и целей электропитания ТСПИ.
* Заземление посторонних проводников и экранов соединительных линий ВТСС.

**Фильтрация**

**🖙** Установка помехоподавляющих фильтров в цепях электропитания ТСПИ.

* Установка разделительных трансформаторов в цепях электропитания ТСПИ.



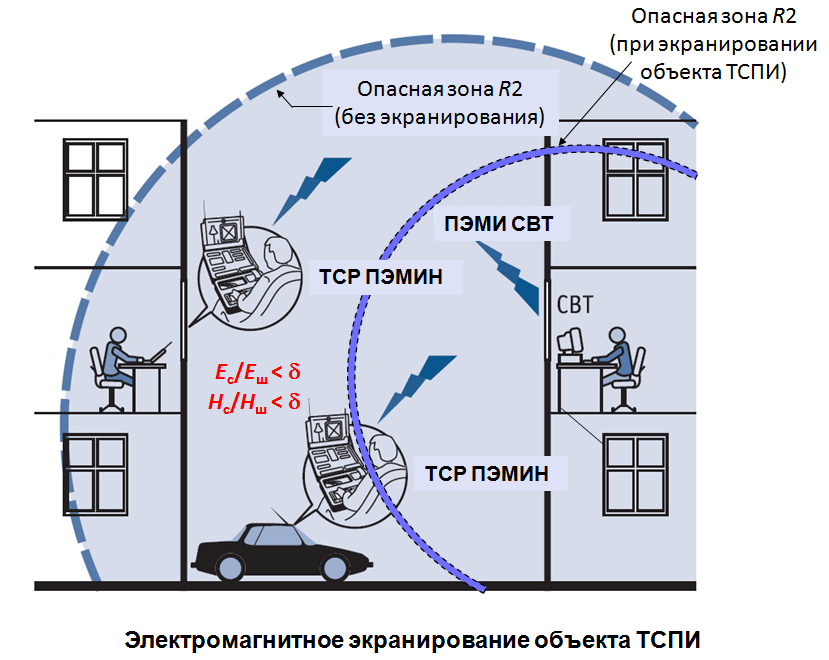
**40.Экранирование и заземление технических средств.**

**Экранирование** - локализация электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами.

Различают три вида *экранирования*:

* электростатическое экранирование заключается в замыкании электростатического поля на поверхность металлического экрана и отводе электрических зарядов на землю (на корпус прибора) с помощью контура заземления;
* магнитостатическое;
* электромагнитное.

При реализации электромагнитного экранирования необходимо заземление экрана источника ПЭМИ, под которым понимается преднамеренное электрическое соединение экрана с заземляющим устройством.



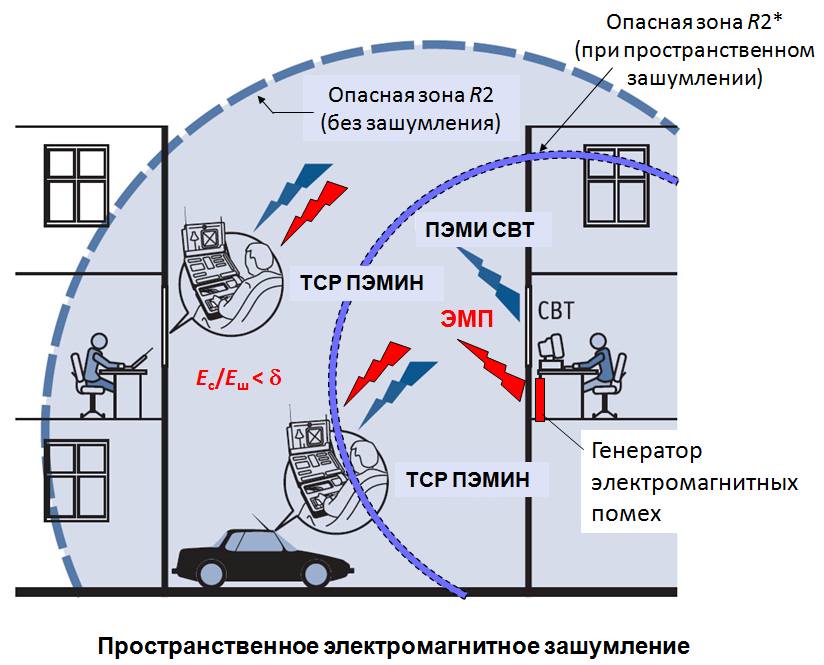
**Заземление** — преднамеренное электрическое соединение какой-либо точки сети с заземляющим устройством.

Защитное действие заземления основано на двух принципах:

* уменьшение до безопасного значения разности потенциалов между заземляемым проводящим предметом и другими проводящими предметами, имеющими естественное заземление
* отвод тока утечки при контакте заземляемого проводящего предмета с фазным проводом

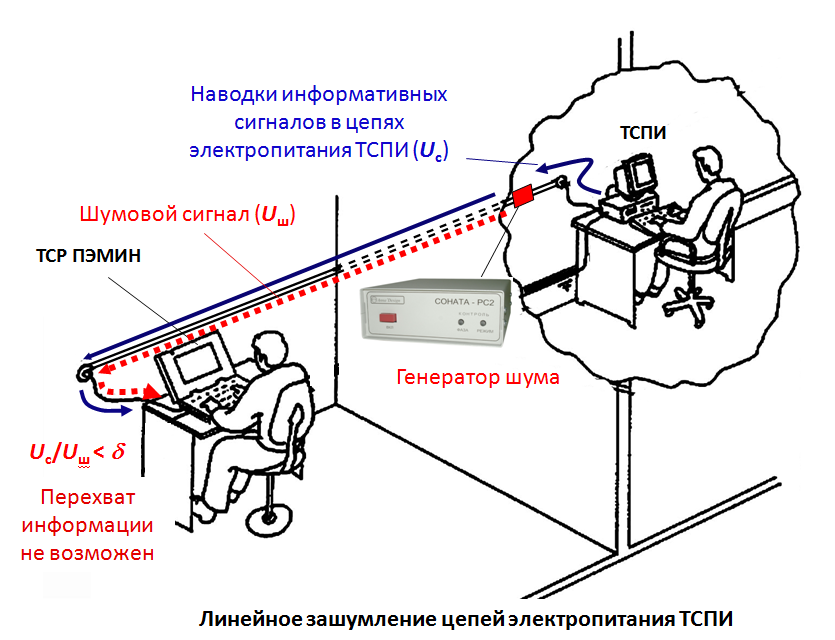
**41.Системы пространственного и линейного электромагнитного зашумления (принцип работы).**

**Система пространственного зашумления** – система, предназначенная для создания маскирующих помех в окружающем пространстве.



В системах пространственного зашумления наиболее широко используются "синфазные помехи" и "белый шум".   
В "синфазных помехах" в качестве сигнала зашумления используются импульсы со случайной амплитудой, синхронизированные с импульсами защищаемого информационного сигнала.  
"Белый шум" представляет собой широкополосный сигнал с равномерным энергетическим спектром во всем рабочем диапазоне частот. Уровень мощности такого сигнала существенно превышает уровень мощности ПЭМИ.

**Система линейного зашумления -** система, предназначенная для маскировки опасных сигналов в ПП и соединительных линиях ВТСС, выходящих за пределы контролируемой территории.

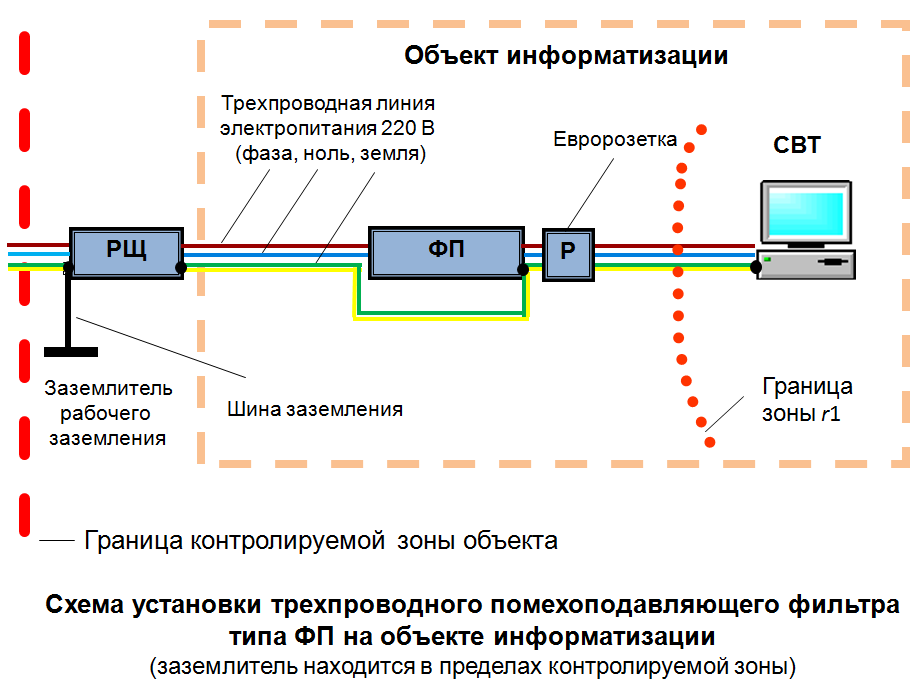


Она представляет из себя генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными характеристиками, который подключается в зашумляемую линию.

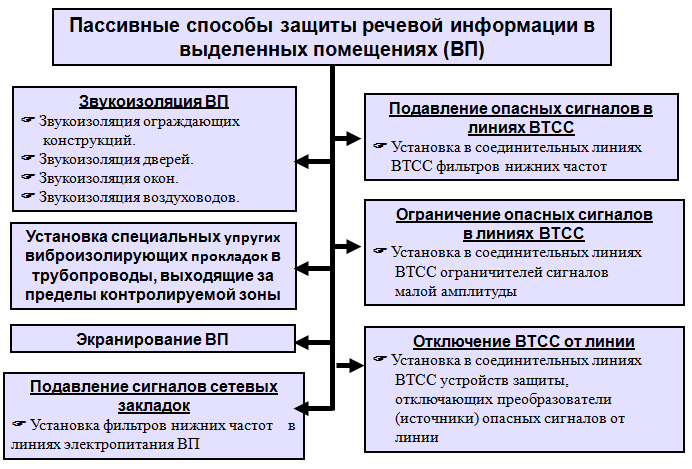
**42.Помехоподавляющие фильтры (принцип работы).**

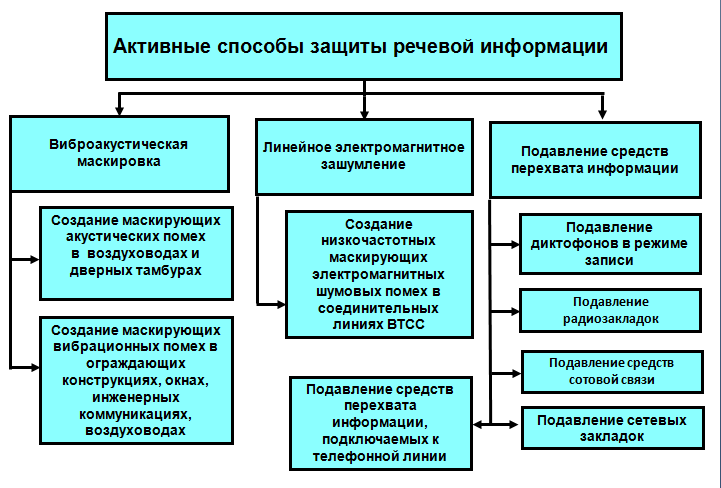
**Помехоподавляющие фильтры –** фильтры, предназначенные для пропускания сигналов с частотами, лежащими в заданной полосе частот, и подавления или ослабления остальных сигналов.

Ниже схема.



**43.Классификация способов и средств защиты акустической речевой информации.**

****

****

**44.Системы виброакустической защиты (принцип работы).**

**Система виброакустической защиты** – система, позволяющая предотвратить возможное прослушивание вибрационных сигналов через оконные стекла, стены, двери, инженерные коммуникации.

**Пассивные средства** – средства, которые ослабляют сигнал от источника информативного сигнала.

**Пассивные** **средства** **виброакустической защиты** – это звукоизоляция помещений, установка виброизолирующих прокладок в трубы. Предназначены для снижения вибрационных сигналов посредством их поглощения.

**Активные средства** - устройства, обеспечивающее создание маскирующих помех или нарушающие нормальное функционирование средств перехвата информации.

**Активные средства виброакустической защиты** – виброакустическое зашумление помещения, стен. Предназначены для маскировки вибрационных сигналов посредством генерации шума большей амплитуды, чем речевая информация.

**45.Средства защиты ВТСС от утечки речевой информации по акустоэлектрическим каналам.**

**Акустоэлектрические каналы утечки информации** – канал утечки, возникающий за счет микрофонного эффекта, например, на катушках индуктивности и звонках телефонных аппаратов появляется модуляция токов, в соответствии с изменениями воздействующих акустических сигналов, которые возможно перехватить, подключившись к линиям ВТСС или телефонной линии.

**Микрофонный эффект** — нежелательное явление, при котором некоторая часть электрической цепи воспринимает звуковые колебания и вибрацию подобно микрофону.



**Пассивные средства** – средства, которые ослабляют сигнал от источника информативного сигнала.

**Пассивные** **средства акустоэлектрической защиты** - экранирование помещения для защиты от высокочастотного облучения,подавление сигналов в линиях ВТСС с помощью фильтров, отключение ВТСС от линии для защиты от прослушивания по проводам и телефонным линиям за пределами КЗ.

**Активные средства** - устройства, обеспечивающее создание маскирующих помех или нарушающие нормальное функционирование средств перехвата информации.

**Активные** **средства акустоэлектрической защиты** – зашумление линий ВТСС для защиты от прослушивания по проводам и телефонным линиям за пределами КЗ.

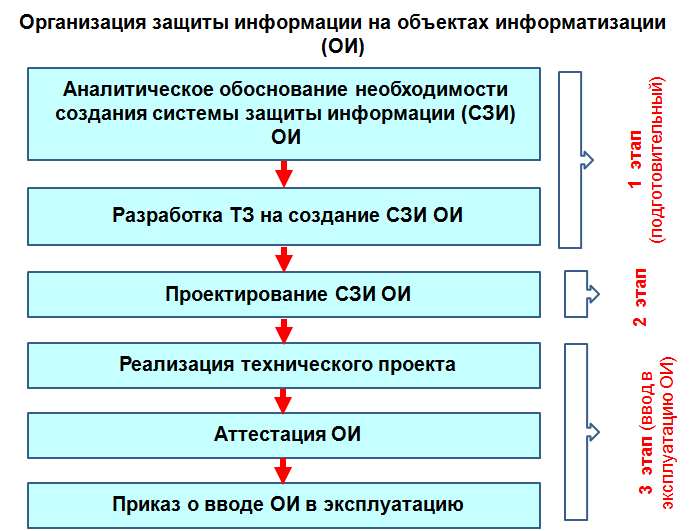
**46.Специальные технические средства подавления средств перехвата речевой информации (подавители диктофонов и широкополосные генераторы шума, блокираторы средств сотовой связи).**

**Специальные технические средства подавления –** средства, предназначенные для подавления различных средств перехвата речевой информации.

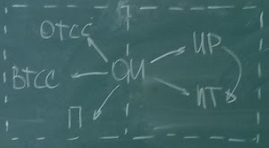
**Подавители диктофонов** – устройства, которое используются для подавления диктофонов. Принцип действия этих устройств основан на генерации мощных шумовых сигналов, которые воздействуют на элементы диктофона, что приводит к значительному искажению записываемой речевой информации.

**Широкополосный генератор шума –** устройство, которое генерирует шум в широком диапазоне, для подавления радиозакладок. Шум приводит к невозможности приема информации от радиозакладок.

**Блокиратор сотовой связи** – устройство, представляющее собой генератор помех, обеспечивающий постановку заградительной помехи в диапазоне рабочих частот приемников телефонов сотовой связи. Помеха приводит к невозможности установления связи и передачи информации от радиозакладок, использующих для передачи информации сети сотовой связи.

**47.Порядок организации защиты информации на объектах информатизации СЗИ.**

**Объект информатизации** – совокупность информационных ресурсов, информационных технологий, ОТСС, ВТСС, персонала и помещений (или объектов) в которых они установлены.



**Средство защиты информации** (СЗИ)— Техническое, программное, программно-техническое средство, вещество или материал, предназначенные или используемые для защиты информации.

**48.Аналитическое обоснование необходимости создания СЗИ.**

**Аналитическое обоснование необходимости создания СЗИ –** документ, в котором

1. Определяется **перечень сведений**, подлежащих защите.
2. Проводится **категорирование** сведений, подлежащих защите.
3. Определяется **перечень лиц**, допущенных до сведений, подлежащих защите.
4. Определяется **степень участия персонала** в обработке информации.
5. Разрабатывается **матрица допуска персонала** к сведениям, подлежащих защите.
6. Определяется **перечень технических средств**, необходимых для обработки конфиденциальной информации (ТСПИ).
7. Осуществляется **выбор помещений для размещения ТСПИ** (ОИ).
8. Осуществляется **выбор помещений для ведения конфиденциальных переговоров** (ВП).
9. Определяется **перечень ВТСС**, необходимых для установки на ОИ.
10. Определяется **модель вероятного нарушителя**.
11. Проводится **специальное обследование** ОИ с целью выявления угроз безопасности информации, разрабатывается **модель угроз**.
12. Проводится **классификация** и **категорирование** ОИ.
13. Разрабатываются **организационные мероприятия** по ЗИ.
14. Определяется **рациональный состав** **средств защиты** для ОИ.
15. Проводится **обоснование необходимости привлечения специализированных организаций** для проектирования и внедрения СЗИ.
16. Проводится **оценка материальных, трудовых и финансовых затрат** на разработку и внедрение СЗИ. Определяются **ориентировочные сроки** разработки и внедрения СЗИ.
17. **Оформляется аналитическое обоснование** необходимости создания СЗИ.
18. Разрабатывается **Техническое задание** на создание СЗИ

**49.Техническое задание на создание СЗИ. Технический проект СЗИ.**

**Технической задание –** это специальный документ, разработанный заказчиком и утвержденный исполнителем, в котором изложены требования, параметры и основные эксплуатационные характеристики объекта или системы**.**

**Техническое задание на разработку СТЗИ (ГОСТ 34.602-89)**

1. Титульный лист.
2. Обоснование разработки.
3. Исходные данные об объекте защиты в техническом, программном, информационном и организационном аспектах.
4. Ссылку на нормативно-методические документы, с учетом которых будет разрабатываться и приниматься в эксплуатацию СТЗИ.
5. Перечень ТСПИ и ВТСС.
6. Конкретные требования к СТЗИ.
7. Перечень предполагаемых к использованию ТСЗИ.
8. Состав, содержание и сроки проведения работ по этапам разработки и внедрения.
9. Перечень подрядных организаций-исполнителей видов работ.
10. Перечень предъявляемой заказчику научно-технической продукции и документации.

**Технический проект -** документ, который разрабатывают с целью определения окончательных технических решений, дающих полное представление об объекте информатизации.

**Состоит из**:

1. титульный лист;
2. пояснительную записку;
3. перечень объектов информатизации, подлежащих защите;
4. перечень выделенных помещений;
5. перечень устанавливаемых ТСПИ с указанием наличия сертификата и мест их установки;
6. перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;
7. перечень устанавливаемых СЗИ с указанием наличия сертификата и мест их установки;
8. схему с указанием плана здания;
9. планы объектов информатизации
10. план – схемы инженерных коммуникаций;
11. план – схемы системы заземления объекта;
12. план – схемы системы электропитания;
13. план – схемы прокладки телефонных линий;
14. план – схемы систем охранной и пожарной сигнализации;
15. план – схемы систем активной защиты;
16. инструкции и руководства по эксплуатации технических средств защиты для пользователей и ответственных за обеспечение безопасности информации на объекте информатизации.

**50.Порядок организации ввода в эксплуатацию СЗИ. Аттестация объекта информатизации.**

**Порядок организации ввода в эксплуатацию СЗИ:**

1. разработка и утверждение организационно-распорядительных документов, определяющих мероприятия по защите информации в ходе эксплуатации системы
2. аттестация системы по требованиям защиты информации
3. мероприятия по реализации технического проекта
4. мероприятия по подготовке персонала к эксплуатации системы

**Аттестация объектов информатизации -** комплекс организационно-технических мероприятий, в результате которых выдается специальный документ - "Аттестата соответствия", который подтверждает, что объект соответствует требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

**Состоит из следующего перечня работ**:

1. анализ исходных данных по ОИ;
2. предварительное ознакомление с ОИ;
3. проведение экспертного обследования ОИ и анализ разработанной документации по защите информации на ОИ;
4. проведение аттестационных испытаний ОИ в реальных условиях эксплуатации;
5. анализ результатов экспертного обследования и аттестационных испытаний ОИ и утверждение заключения по результатам аттестации.