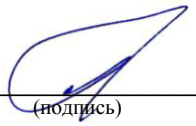
Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

ОДОБРЕНО:

Руководитель программы аспирантуры



_____ А.Н. Привалов
(подпись)

«18» марта 2026 г.

Рабочая программа дисциплины
ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Уровень высшего образования:	Подготовка кадров высшей квалификации
Научная специальность:	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность образовательной программы:	
Срок освоения образовательной программы и форма обучения:	3 года

Шуя

1. Цели освоения дисциплины

Целью учебной дисциплины является содействие аспирантам в приобретении знаний, умений и навыков в области выбора и применения технических методов и средств защиты информации, необходимых в процессе проведения практических работ в рамках диссертационного исследования. В рамках данного курса предполагается изучение основ инженерно-технической защиты информации, а также формирование навыков и умений в области применения этих знаний для конкретных условий.

2. Место дисциплины в структуре ОП

Дисциплина «Технические методы и средства защиты информации» является дисциплиной по выбору блока дисциплин «Дисциплины (модули) по выбору 2 (ДВ.2)».

Успешное освоение данной дисциплины будет способствовать готовности аспирантов к подготовке публикаций и (или) заявок на патенты на изобретения, полезные модели, свидетельства о государственной регистрации программ для электронных вычислительных машин, баз данных, топологий интегральных микросхем, подготовке к прохождению промежуточной аттестации по этапам выполнения научного исследования, итоговой аттестации.

Для освоения данной дисциплины обучающийся должен:

Знать:

– основные нормативно-правовые документы и стандарты в области информационной безопасности;

Уметь:

– работать с документацией, описывающей построенную структуру безопасности информационной системы;

Владеть:

– современной терминологией в области информационной безопасности.

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

Знать:

– основные угрозы нарушения безопасности компьютерных систем и методы их реализации;

– технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

– способы и средства защиты информации, обрабатываемой техническими средствами;

– основы организации технической защиты информации на объектах информатизации в выделенных помещения.

Уметь:

– применять инженерно-технические средства физической защиты объектов информатизации;

– применять технические средства для криптографической защиты информации конфиденциального характера;

– применять технические средства для уничтожения информации и носителей информации;

– применять средства и системы контроля и управления доступом.

Иметь опыт:

– установки и настройки технических средств защиты информации;

– выявления технических каналов утечки информации;

– участия в мониторинге эффективности технических средств защиты информации;

– применения методов и средств контроля эффективности защиты информации от утечки по техническим каналам.

4. Объем и содержание дисциплины

Объем дисциплины составляет 2 зачетных единицы (72 академических часа)

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

№	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в акад. часах, по очной форме обучения)			Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекцион-ного типа	Занятия семинарского типа	Самостоятельная работа обучающихся	
1.	Основные концептуальные положения инженерно-технической защиты информации	3	2	2 практические	4	Практические задания
2.	Виды информации, защищаемой техническими средствами	3	2	2 практические	4	Практические задания
3.	Демаскирующие признаки объектов защиты	3	2	2 практические	4	Практические задания
4.	Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей	3	2	2 практические	4	Практические задания
5.	Виды угроз безопасности информации, защищаемой техническими средствами	3	2	2 практические	4	Практические задания
6.	Принципы добывания и обработки информации техническими средствами	3	2	2 практические	4	Практические задания
7.	Классификация и структура технических каналов утечки информации	3	2	2 практические	4	Практические задания
8.	Средства предотвращения утечки информации по техническим каналам	3	2	2 практические	4	Реферат
9.	Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины	3	2	2 практические	4	Практические задания
10.	Итого за семестр:		18	18	36	Зачет с оценкой

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Тема 1 – Основные концептуальные положения инженерно-технической защиты информации

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

Тема 2 – Виды информации, защищаемой техническими средствами

Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты. Семантическая информация, циркулирующая в человеческом обществе. Профессиональные языки. Признаковая информация. Информация о видовых признаках, о признаках сигналов, о признаках веществ. Структурирование информации.

Тема 3 – Демаскирующие признаки объектов защиты

Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности. Видовые демаскирующие признаки. Демаскирующие признаки сигналов. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.

Тема 4 – Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей

Виды источников и носителей информации. Прямые и косвенные источники семантической информации. Принципы записи и съема информации с её носителя. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции. Побочные электромагнитные излучения и наводки.

Тема 5 – Виды угроз безопасности информации, защищаемой техническими средствами

Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий. Технические каналы утечки информации: наблюдение, подслушивание, перехват. Источники угроз безопасности информации. Опасные сигналы и их источники.

Тема 6 – Принципы добывания и обработки информации техническими средствами

Способы и средства наблюдения в оптическом диапазоне. Обработка информации в оптическом приемнике. Способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов. Обработка информации в радиоприемнике. Способы и средства подслушивания. Обработка информации в акустическом приемнике.

Тема 7. Классификация и структура технических каналов утечки информации

Типовая структура и виды технических каналов утечки информации. Каналы утечки речевой информации. Каналы утечки информации при её передаче по каналам связи. Каналы утечки видовой информации. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений. Каналы утечки информации за счет побочных электромагнитных излучений и наводок.

Тема 8 – Средства предотвращения утечки информации по техническим каналам

Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления.

Тема 9 – Заключительный. Подведение и анализ промежуточных результатов освоения дисциплины

5. Образовательные технологии

В программе данного курса предусмотрено использование в учебном процессе активных форм проведения занятий и организации самостоятельной работы. В учебном процессе

предусмотрено использование технологий проблемного обучения, а также предметно-ориентированных технологий обучения, таких как: технология экспертной оценки состояния информационной безопасности; технология дистанционного анализа уязвимостей АИС; технология математического моделирования конфликтных ситуаций; технология процессного анализа состояния ИБ.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения, мультимедиа технологии, облачные технологии, технологии визуализации (инфографика, дашборды).

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся по дисциплине осуществляется в следующих формах:

– повторение материала с использованием конспектов лекций;

– изучение и анализ предложенных электронных образовательных ресурсов, содержащих информацию по техническим методам и средствам защиты информации;

– выполнение заданий, из которых складывается портфолио студента, включающее обязательные и дополнительные (определяемые студентами совместно с преподавателем) материалы.

Задания и результаты их выполнения составляют часть информационного ресурса кафедры математики, информатики и методики обучения и хранятся на сервере кафедры, доступ к ним обеспечен с компьютеров в компьютерном классе.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в приложении 1 к настоящей программе. Доступ к методическим материалам осуществляется при помощи электронной информационно-образовательной среды Шуйского филиала ИвГУ.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Промежуточная аттестация по дисциплине (зачет с оценкой) проводится с использованием рейтинговой оценки.

Промежуточная аттестация аспирантов предполагает зачет с оценкой в форме выполнения тестового задания, примерный вариант которого представлен в Приложении 2.

Критерии оценки:

– оценка «отлично» выставляется аспиранту, если аспирант выполнил тестового задание на 85 или более процентов;

– оценка «хорошо» выставляется аспиранту, если аспирант выполнил тестового задание на 71 или более процентов;

– оценка «удовлетворительно» выставляется аспиранту, если аспирант выполнил тестового задание на 61 или более процентов;

– оценка «неудовлетворительно» выставляется аспиранту, если аспирант выполнил тестовое задание на менее чем 61 процент;

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. – 7-е изд., испр. – Москва : Горячая линия – Телеком, 2012. – 442 с. : ил. – ISBN 978-5-9912-0233-6; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=253208

2. Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д. А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. URL: http://biblioclub.ru/index.php?page=book&id=429070

3. Громов, Ю. Ю. Организация безопасной работы информационных систем [Электронный ресурс] : учеб. пособие для студентов / Ю. Ю. Громов. - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. URL: http://biblioclub.ru/index.php?page=book&id=277794

4. Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с.; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=208661

Дополнительная литература:

1. Данилова, О. Т. Технические средства разведки и защита информации : учебное пособие : в 4 частях : / О. Т. Данилова ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2019. – Часть 1. Технические каналы утечки речевой акустической конфиденциальной информации. – 64 с. : ил., табл., схем., граф. – ISBN 978-5-8149-2838-2; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=682094

2. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 256 с. : схем., табл., ил. - Библиогр.: с. 213. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480636

3. Семенихина, Д. В. Теоретические основы радиоэлектронной борьбы. Радиоэлектронная разведка и радиоэлектронное противодействие : учебное пособие / Д. В. Семенихина, Ю. В. Юханов, Т. Ю. Привалова ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону : Южный федеральный университет, 2015. – 252 с. : ил. – ISBN 978-5-9275-1815-9; То же [Электронный ресурс]. – URL: https://biblioclub.ru/index.php?page=book&id=445197

4. Артемов, А. В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605

5. Иванов, А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие : / А. В. Иванов, В. А. Трушин ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2012. – 43 с. : ил.,табл., схем. – ISBN 978-5-7782-1888-8; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=228846

6. Галатенко, В. А. Основы информационной безопасности : курс лекций : учебное пособие / В. А. Галатенко ; Интернет университет информационных технологий ; под ред. В. Б. Бетелина. - 2-е изд. ; испр. - Москва : Интернет-Университет Информационных Технологий, 2006. - 208 с. - URL: http://biblioclub.ru/index.php?page=book&id=233063

7. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

8. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

9. Информационная безопасность : учебно-методические материалы для проведения практических занятий / Министерство образования и науки РФ; ГОУ ВПО "Шуйский государственный педагогический университет" ; авт.-сост. А. А. Михайлов, Г. Д. Хубулов. - Шуя : Изд-во ГОУ ВПО "ШГПУ", 2010. - 56 с.

10. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - М. : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). - ISBN 978-5-00046-137-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774

Ресурсы информационно-телекоммуникационной сети «Интернет»:
Профессиональные базы данных и информационно-справочные системы:
ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
Национальный цифровой ресурс Руконт - https://rucont.ru/default.aspx
Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru
Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;
- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: электронные пособия (презентации), аудио-визуальные пособия (видеоматериалы), печатные пособия (таблицы, схемы)).

Автор(ы) рабочей программы дисциплины: профессор кафедры математики, информатики и методики обучения, доктор технических наук, профессор Привалов А. Н.

Программа рассмотрена и утверждена на заседании кафедры математики, информатики и методики обучения «02» марта 2022 г., протокол № 8

Программа обновлена
протокол заседания кафедры № 8 от «22» марта 2023 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 7 от «9» февраля 2024 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 9 от «20» марта 2025 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Программа обновлена
протокол заседания кафедры № 9 от «18» марта 2026 г.
Согласовано:
Руководитель ОП _____ А.Н. Привалов
(подпись)

Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Шуйский филиал ИвГУ

Кафедра математики, информатики и методики обучения

Приложение 1
к рабочей программе дисциплины

Методические указания
для обучающихся по освоению дисциплины
ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Уровень высшего образования:	Подготовка кадров высшей квалификации
Научная специальность:	2.3.6. Методы и системы защиты информации, информационная безопасность
Направленность образовательной программы:	
Срок освоения образовательной программы:	3 года

Шуя

1. Методические указания к проработке лекционного материала по дисциплине

Общий план лекций включает следующие составные элементы:

Название этапа	**Содержание**	**Время, мин.**
Вступительная часть	Приветствие. Контроль посещаемости. Постановка темы, цели, основных задач.	4-7
Актуальность и основные понятия	Формулирование проблемы; основные понятия и суть изучаемого вопроса.	8-10
Основная часть	Представление материала лекции в соответствии с программой	60-65
Закрепление полученной информации	Вопрос-ответ, фронтальный опрос, разбор ошибок, допущенных при ответах	5-8
Подведение итогов	Сопоставление результатов лекции с установленной целью и намеченными задачами.	3

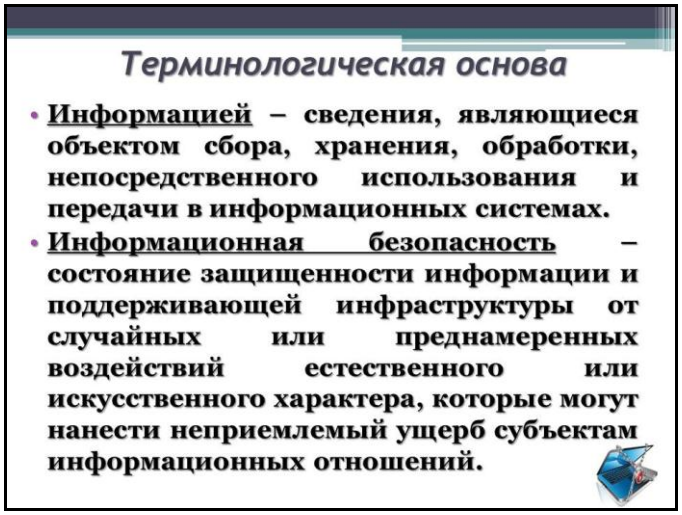
В рамках проведения занятий по дисциплине предполагается чтение следующих лекций:

Лекция 1. Основные концептуальные положения инженерно-технической защиты информации

Тезисы лекции:

- Цели и задачи защиты информации.
- Ресурсы, выделяемые на защиту информации.
- Принципы защиты информации техническими средствами.
- Основные направления инженерно-технической защиты информации.
- Показатели эффективности инженерно-технической защиты информации.

Слайды презентации к лекции:



Терминологическая основа

- **Защита информации – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.**



Информационная угроза

Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации.

Концепция информационной безопасности, в общем случае, должна отвечать на три вопроса:

- Что защищать?
- От чего (кого) защищать?
- Как защищать?





В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

- **Конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;**
- **Целостность – избежание несанкционированной модификации информации;**
- **Доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.**

Цели защиты информации

1. **Соблюдение конфиденциальности информации ограниченного доступа.**
2. **Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к такой информации.**
3. **Предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию и предоставлению информации, а также иных неправомерных действий в отношении такой информации.**
4. **Реализация конституционного права граждан на доступ к информации.**
5. **Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.**

Принципы защиты информации

1. **Комплексность.**
2. **Своевременность.**
3. **Непрерывность**
4. **Активность.**
5. **Законность.**
6. **Обоснованность.**
7. **Специализация.**
8. **Совершенствование.**
9. **Централизация управления.**
10. **Экономическая целесообразность.**
11. **Взаимодействие и координация деятельности.**



Инженерно-техническая защита информации

Инженерно-техническая защита (ИТЗ) — это совокупность специальных органов, технических средств и мероприятий по их использованию в целях защиты конфиденциальной информации.

Она решает следующие ***задачи:***

1. Предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или изменения.
2. Защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении.
3. Предотвращение утечки информации по различным техническим каналам.

Эффективность инженерно-технической защиты информации

Для обеспечения эффективной инженерно-технической защиты информации ***необходимо определить***:

- **что защищать** техническими средствами в конкретной организации, здании, помещении;
- **каким угрозам подвергается** защищаемая информация со стороны злоумышленников и их технических средств;
- **какие способы и средства** целесообразно применять для обеспечения безопасности информации с учетом как величины угрозы, так и затрат на ее предотвращение;
- **как организовать и реализовать** техническую защиту информации в организации.

Принципы инженерно-технической защиты информации

В основу защиты должны быть положены следующие принципы, аналогичные принципам добывания, а именно:

- ***непрерывность*** защиты информации, характеризующая постоянную готовность системы защиты к отражению угроз безопасности информации в любое время;
- ***активность***, предусматривающая прогнозирование действий злоумышленника, разработку и реализацию опережающих мер по защите;
- ***скрытность***, исключающая ознакомление посторонних лиц со средствами и технологией защиты информации;
- ***целеустремленность***, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценной информации;
- ***комплексное использование*** различных способов и средств защиты информации, позволяющая компенсировать недостатки одних достоинствами других.

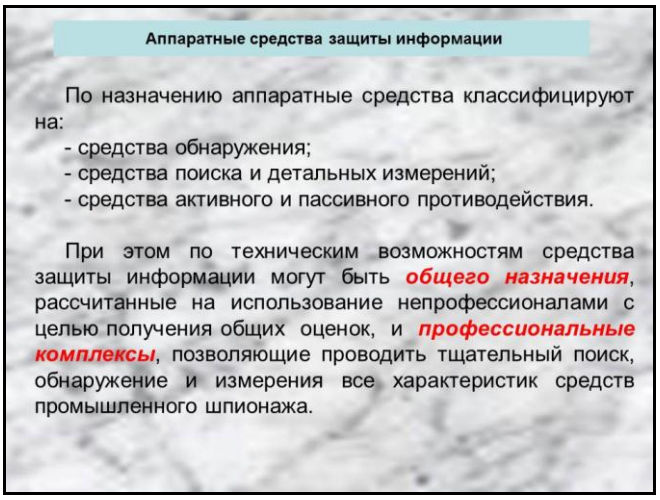
Физические средства защиты

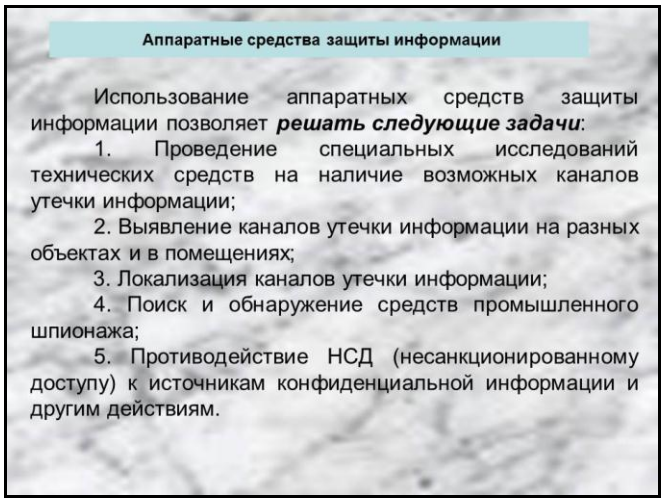
В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на ***следующие группы***:

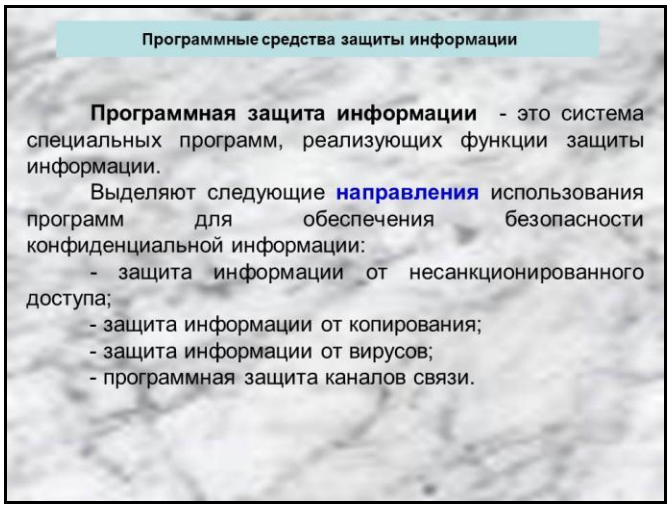
- охранные и охранно-пожарные системы;
- охранное телевидение;
- охранное освещение;
- средства физической защиты.

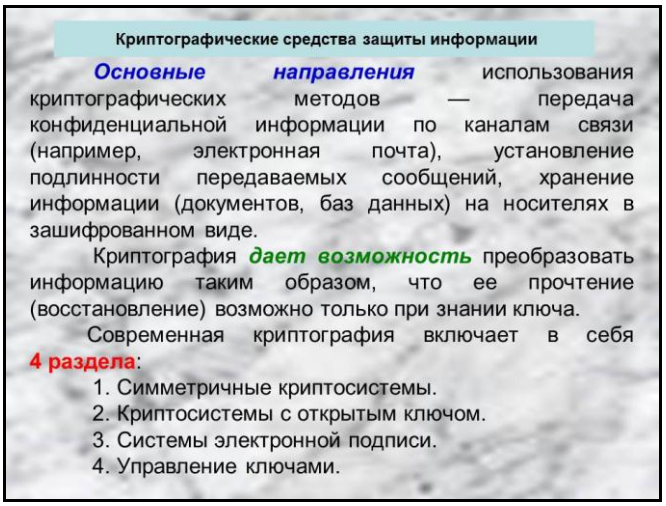
Эти средства применяются ***для решения следующих задач***:

1. охрана территории предприятия и наблюдение за ней;
2. охрана зданий, внутренних помещений и контроль за ними;
3. охрана оборудования, продукции, финансов и информации;
4. осуществление контролируемого доступа в здания и помещения.


Аппаратные средства защиты информации
По назначению аппаратные средства классифицируют на:
- средства обнаружения;
- средства поиска и детальных измерений;
- средства активного и пассивного противодействия.
При этом по техническим возможностям средства защиты информации могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения общих оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и измерения все характеристик средств промышленного шпионажа.


Аппаратные средства защиты информации
Использование аппаратных средств защиты информации позволяет решать следующие задачи:
1. Проведение специальных исследований технических средств на наличие возможных каналов утечки информации;
2. Выявление каналов утечки информации на разных объектах и в помещениях;
3. Локализация каналов утечки информации;
4. Поиск и обнаружение средств промышленного шпионажа;
5. Противодействие НСД (несанкционированному доступу) к источникам конфиденциальной информации и другим действиям.


Программные средства защиты информации
Программная защита информации - это система специальных программ, реализующих функции защиты информации.
Выделяют следующие направления использования программ для обеспечения безопасности конфиденциальной информации:
- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита информации от вирусов;
- программная защита каналов связи.



Литература: Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с.; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=208661

Лекция 2. Виды информации, защищаемой техническими средствами

Тезисы лекции:

- Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.
- Семантическая информация, циркулирующая в человеческом обществе.
- Профессиональные языки.
- Признаковая информация.
- Информация о видовых признаках, о признаках сигналов, о признаках веществ. Структурирование информации.

Иллюстративный материал к лекции:



Введение

Информационной безопасностью называют комплекс организационных, технических и технологических мер по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

ИБ дает гарантию того, что достигаются следующие цели:

- ***конфиденциальность*** информации (свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц);
- ***целостность*** информации и связанных с ней процессов (неизменность информации в процессе ее передачи или хранения);
- ***доступность*** информации, когда она нужна (свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию).

Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г.

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Что является **объектом** защиты?
Что составляет **предмет** защиты?

Подведение итогов



Обеспечение **безопасности информации** складывается из трех составляющих:

- Конфиденциальности,
- Целостности,
- Доступности.

Точками приложения процесса защиты информации к информационной системе являются:

- аппаратное обеспечение,
- программное обеспечение
- обеспечение связи (коммуникации).

Сами процедуры(механизмы) защиты разделяются на

- защиту физического уровня,
- защиту персонала
- организационный уровень.

Всякую ли информацию требуется защищать?

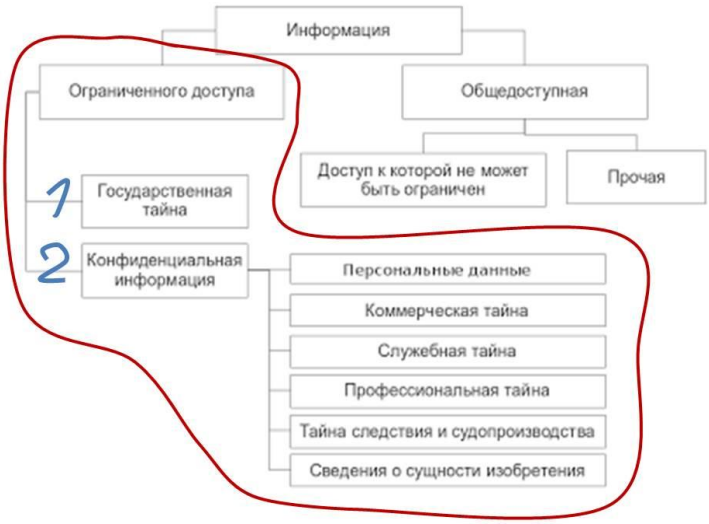
Ценность информации – главный критерий по ее защите

Признаки защищаемой информации

- Ограниченный доступ
- Чем важнее информация, тем сильнее ее защита в соответствии с присвоенной ей степенью секретности
- Защищаемая информация должна иметь определенную ценность и приносить пользу ее собственнику, оправдывая затрачиваемые на ее защиту силы и средства

Информация как предмет защиты

Согласно российскому законодательству – **Федеральному закону РФ от 27 июля 2006 г. N 149-ФЗ** «Об информации, информационных технологиях и о защите информации» информация подразделяется (в зависимости от категории доступа к ней) на **общедоступную** информацию и **информацию, доступ к которой ограничен** федеральными законами (Ст.5).



Информация, к которой нельзя ограничивать доступ

Перечень сведений, доступ к которым не может быть ограничен, указан в Ст.10 того же ФЗ РФ от 27 июля 2006 г. N 149 "Об информации...":

- нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды;
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных ИС, созданных или предназначенных для обеспечения граждан и организаций такой информацией;
- иной информации (напр. о благотворительной деятельности и некоммерческих организациях), недопустимость ограничения доступа к которой установлена федеральными законами.

Информация ограниченного доступа: 1. Государственная тайна

Государственная тайна — защищаемые государством сведения, распространение которых может нанести ущерб безопасности РФ

Регулирование вопросов, связанных с этим видом тайн возложено на Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне". Перечень сведений составляющих гос. тайну определен в Ст.5, где они сгруппированы по следующим направлениям:

1. сведения в **военной области**
2. сведения в **области экономики, науки и техники**
3. сведения в **области внешней политики и экономики**
4. сведения в области **разведывательной**, **контрразведывательной** и **оперативно-розыскной** деятельности, а также в **области противодействия терроризму**

Информация ограниченного доступа: 2. Конфиденциальная информация

Перечень сведений конфиденциального характера опубликован в Указе Президента РФ от 6 марта 1997 г. N 188 « Об утверждении перечня сведений конфиденциального характера». К видам конфиденциальной информации, согласно этому указу относятся:

- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (**персональные данные**), за исключением сведений, подлежащих распространению в СМИ в установленных ФЗ случаях.
- Сведения, составляющие **тайну следствия и судопроизводства**, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с ФЗ от 20 августа 2004 г. N 119-ФЗ " О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства " и др. нормативными правовыми актами РФ.
- Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (**служебная тайна**).
- **Сведения, связанные с профессиональной деятельностью**, доступ к которым ограничен в соответствии с Конституцией РФ и ФЗ (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.).
- Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и ФЗ (**коммерческая тайна**).
- **Сведения о сущности изобретения**, полезной модели или промышленного образца до официальной публикации информации о них.

Коммерческая тайна — это информация, которая имеет действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и к которой принимаются меры по охране конфиденциальности. Она охраняется при содействии государства.

Обладатели коммерческой тайны — физические (независимо от гражданства) и юридические (коммерческие и некоммерческие организации) лица, занимающиеся предпринимательской деятельностью и имеющие монопольное право на информацию, составляющую для них коммерческую тайну.

Правопреемники — это физические и юридические лица, которым в силу служебного положения, по договору или на ином законном основании (в том числе по наследству) известна информация, составляющая коммерческую тайную другого лица

Профессиональная тайна — защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам держателя или другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной

Информация может быть отнесена к категории профессиональной тайны, если она соответствует следующим требованиям:

- Информация не относится к сведениям, составляющим государственную и коммерческую тайну
- Информация стала известной или была доверена лицу лишь в силу исполнения им своих профессиональных обязанностей
- Информация стала известной или была доверена лицу, не состоящему на государственной или муниципальной службе (в противном случае информация считается служебной тайной)

В соответствии с федеральным законом имеется запрет на распространение доверенной или ставшей известной информации, которая может нанести ущерб правам и законным интересам доверителя

В соответствии с этими критериями можно выделить следующие **объекты профессиональной тайны:**

- врачебная тайна
- нотариальная тайна
- адвокатская тайна
-тайна связи
- тайна страхования
- тайна исповеди
- банковская тайна

Служебная тайна — защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости

Объекты служебной тайны:

- служебная информация о деятельности федеральных государственных органов, доступ к которой ограничен федеральным законом в целях защиты государственных интересов
- охраноспособная конфиденциальная информация, ставшая известной в силу исполнения служебных обязанностей должностным лицом государственных органов и органов местного самоуправления

Информация, относящаяся к категории служебной тайны, должна отвечать следующим критериям:

- являться собственной служебной тайной
- являться охраноспособной конфиденциальной информацией служебного характера (чужой тайной) другого лица
- не являться государственной тайной и не входить в перечень сведений, доступ к которым не может быть ограничен
- Должна быть получена представителем государственного органа и органа местного самоуправления только в силу исполнения обязанностей по службе в случаях и порядке, установленных федеральным законом

Информация, не отвечающая этим требованиям, не может считаться служебной тайной и не подлежит правовой охране

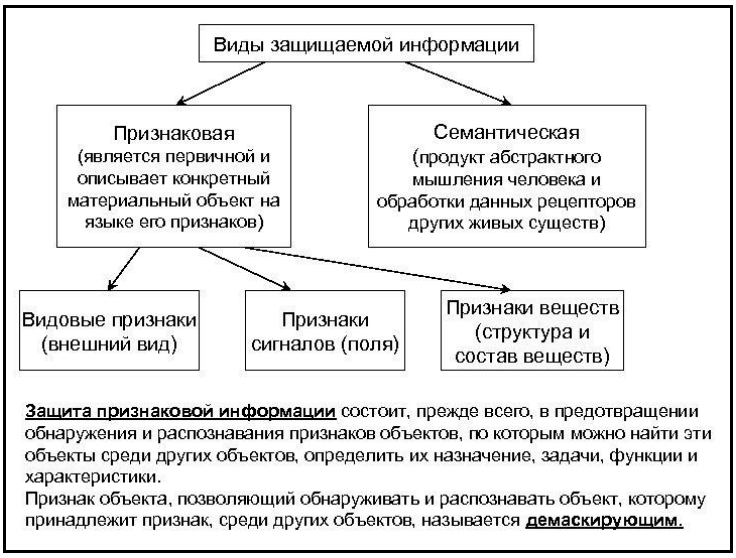
Персональные данные – сведения, использование которых без согласия субъекта персональных данных может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам:

- биографические и опознавательные данные
- сведения о семейном положении
- сведения об имущественном, финансовом положении
- личные характеристики
- сведения о состоянии здоровья

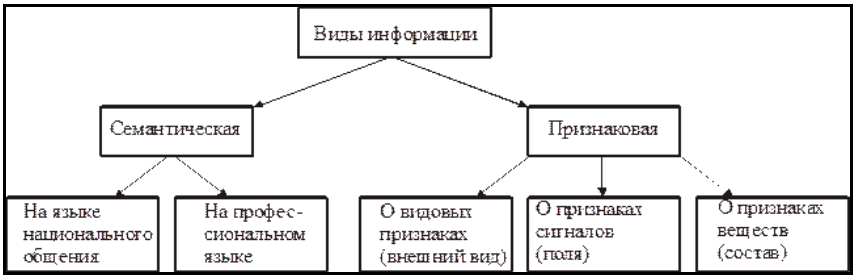
Субъектами права здесь выступают:
- лица, к которым относятся соответствующие данные, и их наследники;
- держатели персональных данных

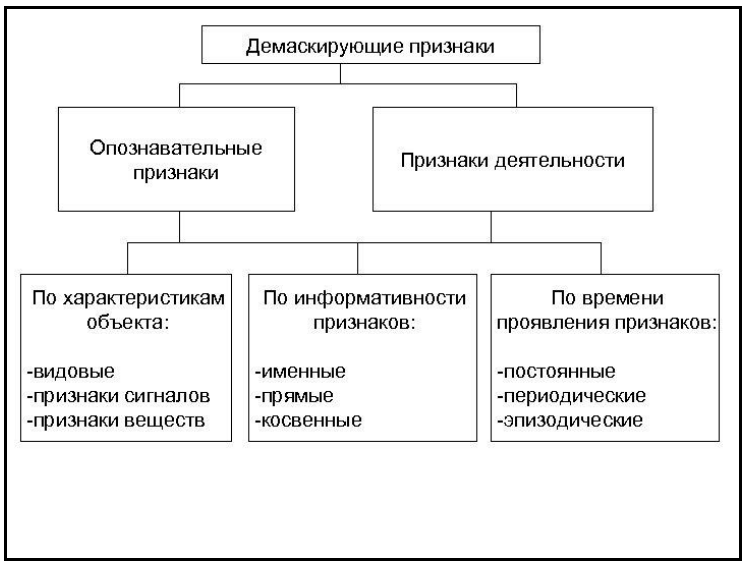
К числу основных **объектов интеллектуальной собственности** *относятся:*

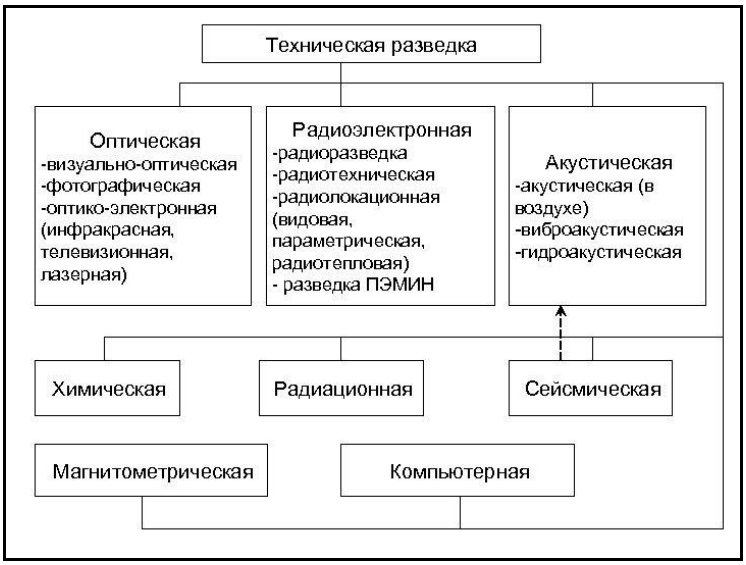
- произведения науки, литературы и искусства;
- результаты исполнительской деятельности артистов, режиссеров, дирижеров;
- результаты творчества;
- звукозаписи и записи изображения
- передача радио- и телевизионных сигналов
- изобретения
- промышленные образцы
- профессиональные секреты (ноу-хау)
- полезные модели
- селекционные достижения
- фирменные наименования и коммерческие обозначения правообладателя;
- товарные знаки и знаки обслуживания
- наименования мест происхождения товаров
- другие результаты интеллектуальной деятельности и средства индивидуализации, на которые в соответствии с законом могут признаваться или закрепляться исключительные права



Защита признаковой информации состоит, прежде всего, в предотвращении обнаружения и распознавания признаков объектов, по которым можно найти эти объекты среди других объектов, определить их назначение, задачи, функции и характеристики.
Признак объекта, позволяющий обнаруживать и распознавать объект, которому принадлежит признак, среди других объектов, называется **демаскирующим.**







Литература: Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д. А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. URL: http://biblioclub.ru/index.php?page=book&id=429070

Лекция 3. Демаскирующие признаки объектов защиты

Тезисы лекции:

- Классификация демаскирующих признаков.
- Опознавательные признаки и признаки деятельности.
- Видовые демаскирующие признаки.
- Демаскирующие признаки сигналов.
- Демаскирующие признаки веществ.
- Именные, прямые и косвенные демаскирующие признаки.

Слайды презентации к лекции:



- Технический демаскирующий признак объекта – характерное свойство объекта защиты, которое может быть использовано технической разведкой для обнаружения и распознавания объекта, а также для получения необходимых сведений о нем.
- Обнаружение объекта – процесс функционирования средства технической разведки, в результате которого фиксируются технические демаскирующие признаки объекта и делается заключение о его наличии.

Основные типы:

- расположения – признак, определяющий положение объекта среди других объектов и предметов окружающего пространства;
- структурно-видовой – признак, определяющий структуру и видовые характеристики группового объекта (состав, количество и расположение отдельных объектов, форму и геометрические размеры);
- деятельности – признак, раскрывающий функционирование объекта через физические проявления.

Основные классы демаскирующих признаков

- **прямые демаскирующие признаки** – признаки, связанные с функционированием объекта защиты и проявляющиеся через их физические поля (электромагнитные, акустические, радиационные и т.п.), отличающиеся по уровню на фоне физических полей окружающей среды, не связанных с защищаемой информацией;
- **косвенные демаскирующие признаки** – признаки, в основе которых лежат последствия изменения окружающей среды как результат функционирования объекта (визуально-оптические признаки деятельности, геометрические размеры, контрастность освещенности, следы производственной деятельности и функционирования и т.п.)

Классификация ДП



ДП в видимом диапазоне ЭМ спектра

Контраст

Контраст по яркости определяется как:

$$K = \frac{B_{max} - B_{\min}}{B_{\max}}$$

Bmin – Минимальная яркость
Bmax – Максимальная яркость

К	
менее 20%	Незаметный контраст
от 20 до 30%	Малозаметный контраст
от 30 до 60%	Заметный контраст
более 60%	Резкозаметный контраст





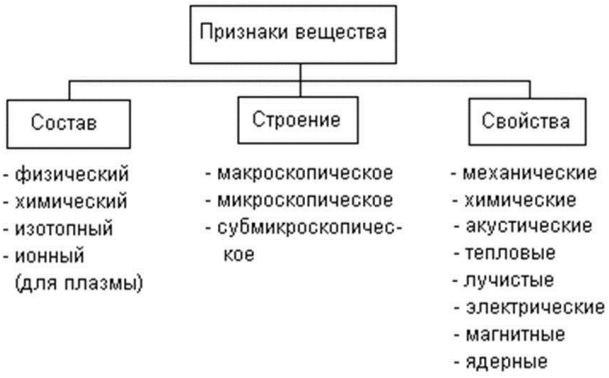


Ответ: Изображение Леопард-2 в ИК диапазоне после длительного пробега. Отчетливо виден нагрев двигателя, гусениц и катков.

Сигнальные демаскирующие признаки

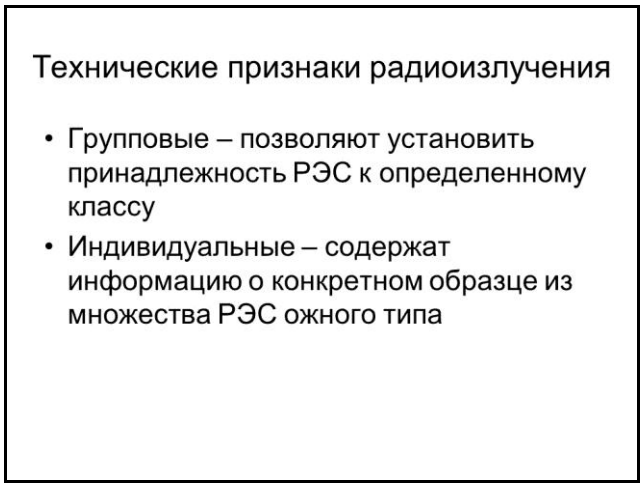


Вещественные демаскирующие признаки



ДП радиоэлектронных средств

- Частотные
- Временные
- Энергетические
- Спектральные
- Пространственно-энергетические
- Фазовые
- Поляризационные



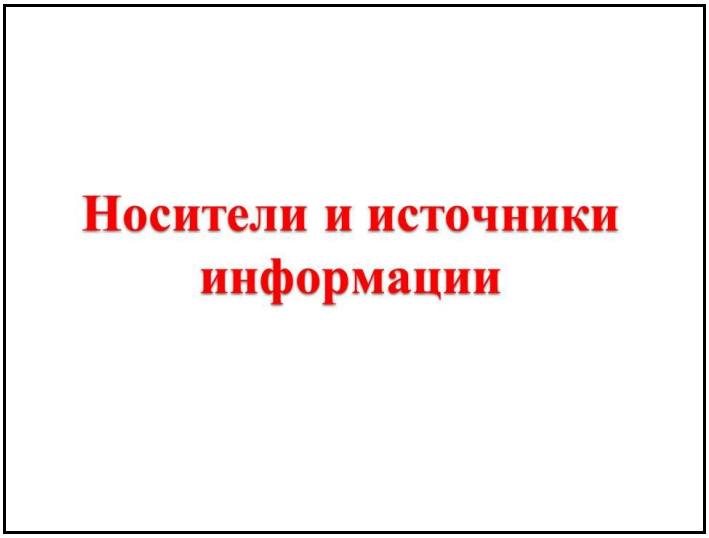
Литература: Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д. А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. URL: http://biblioclub.ru/index.php?page=book&id=429070

Лекция 4. Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей

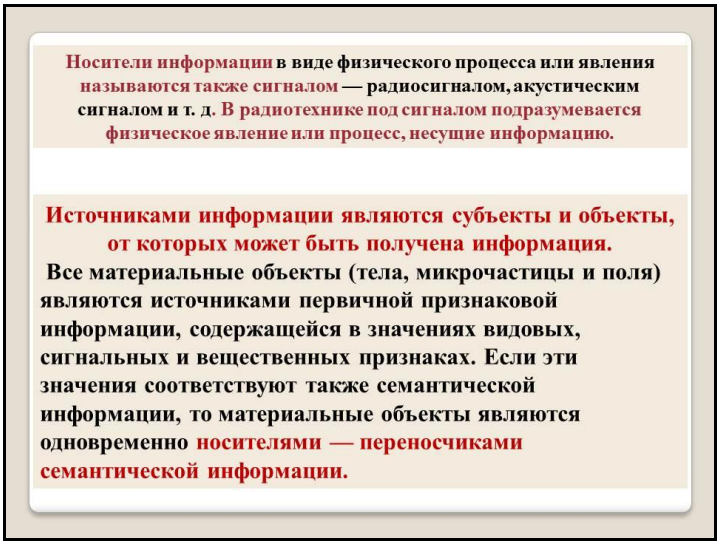
Тезисы лекции:

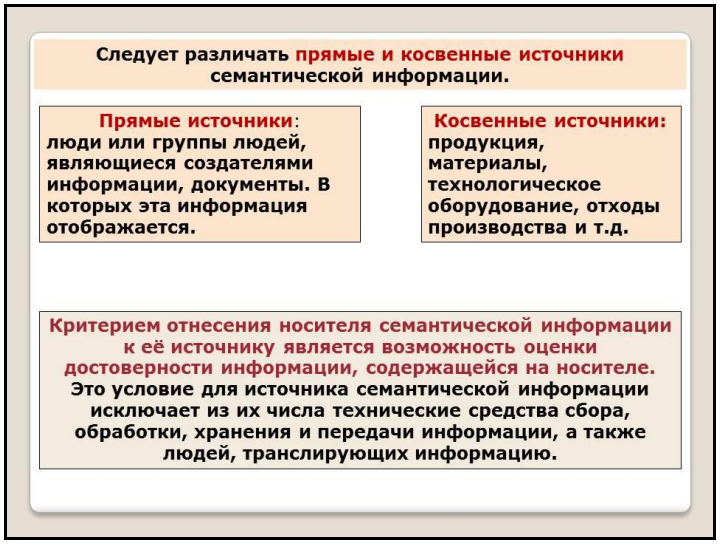
- Виды источников и носителей информации.
- Прямые и косвенные источники семантической информации.
- Принципы записи и съема информации с её носителя.
- Источники функциональных сигналов.
- Понятие модуляции, манипуляции, демодуляции.
- Побочные электромагнитные излучения и наводки.

Слайды презентации к лекции:




Широко применяемое понятие «носитель информации» имеет разнообразный смысл. Например, человек как носитель информации, учебник, магнитный или бумажный носитель, магнитное поле, электрический ток и др.
Носители признаковой информации целесообразно обозначить как первичные. Такими носителями являются:
Макротела
Поля
Микрочастицы (элементарные частицы)
Папирус, глина, береста, камень, бумага. Машинные носители: магнитные, полупроводниковые, светочувствительные, и другие
Акустические Электрические, магнитные, электромагнитные (в диапазоне видимого и ИК света, в радиодиапазоне).
Электроны и ядра гелия
Гибкий или жесткий диск, магнитная лента..
Вторичные носители


Носители информации в виде физического процесса или явления называются также сигналом — радиосигналом, акустическим сигналом и т. д. В радиотехнике под сигналом подразумевается физическое явление или процесс, несущие информацию.
Источниками информации являются субъекты и объекты, от которых может быть получена информация.
Все материальные объекты (тела, микрочастицы и поля) являются источниками первичной признаковой информации, содержащейся в значениях видовых, сигнальных и вещественных признаках. Если эти значения соответствуют также семантической информации, то материальные объекты являются одновременно носителями — переносчиками семантической информации.


Следует различать прямые и косвенные источники семантической информации.
Прямые источники: люди или группы людей, являющиеся создателями информации, документы. В которых эта информация отображается.
Косвенные источники: продукция, материалы, технологическое оборудование, отходы производства и т.д.
Критерием отнесения носителя семантической информации к её источнику является возможность оценки достоверности информации, содержащейся на носителе. Это условие для источника семантической информации исключает из их числа технические средства сбора, обработки, хранения и передачи информации, а также людей, транслирующих информацию.

Под документом понимается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. К документам относится служебная информация, научные публикации в открытой и закрытой печати, статьи в газетах и журналах о деятельности организации или ее сотрудников, реклама, отчеты сотрудников, конструкторская и технологическая документация и т. д.

Документы относятся к наиболее информативным источникам, так как они содержат, как правило, достоверную информацию в отработанном и сжатом виде, в особенности если документы подписаны или утверждены.

ВНИМАНИЕ!

Технические средства сбора, обработки, хранения и передачи информации нельзя отнести к источникам семантической информации, так как они представляют собой лишь инструмент для преобразования входной информации.

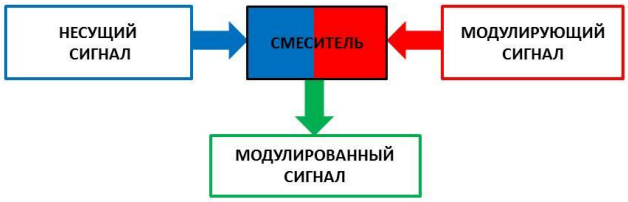
Запись и съем информации с ее носителя.

Материализация (запись) любой информации производится путем изменения параметров носителя. Механизм запоминания и воспроизведения информации человеком в настоящее время еще недостаточно изучен и нет однозначного и ясного представления о носителях информации в мозгу человека.

Запись информации на материальные тела производится путем изменения их физической структуры и химического состава.

Запись информации на носители в виде полей и электрического тока осуществляется путем изменения их параметров. Непрерывное изменение параметров сигналов в соответствии со значениями первичного сигнала называется модуляцией, дискретное — манипуляцией. Первичным является сигнал от источника информации.

ОБЩИЕ ПОНЯТИЯ О МОДУЛЯЦИИ



Модуляцией называется процесс изменения одного из параметров ВЧ сигнала в соответствии с передаваемым сообщением.

ОБЩИЕ ПОНЯТИЯ О МОДУЛЯЦИИ

$$A(t) = A_0 \sin(\omega_0 t + \varphi_0)$$

A_0 амплитуда гармонического колебания;

ω_0 частота гармонического колебания;

φ_0 фаза гармонического колебания.

- ГАРМОНИЧЕСКИЙ СИГНАЛ (УЗКИЙ СПЕКТР)
  - АНАЛОГОВАЯ МОДУЛЯЦИЯ
  - ЦИФРОВАЯ МОДУЛЯЦИЯ

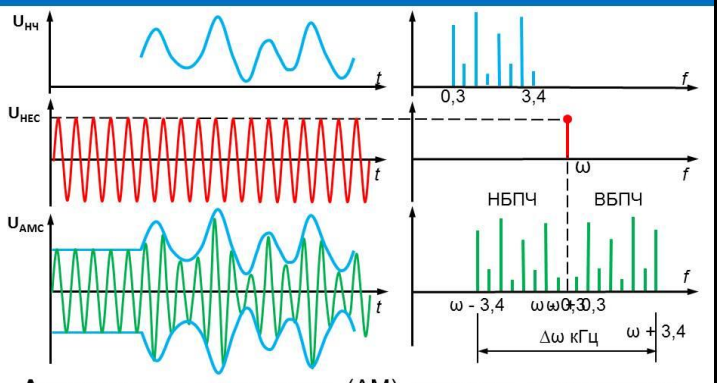
ОСНОВНЫЕ ХАРАКТЕРИСТИКИ МОДУЛЯЦИИ

- ЭНЕРГЕТИЧЕСКАЯ ЭФФЕКТИВНОСТЬ
- СПЕКТРАЛЬНАЯ ЭФФЕКТИВНОСТЬ
- УСТОЙЧИВОСТЬ К ВОЗДЕЙСТВИЯМ КАНАЛА ПЕРЕДАЧИ
- ТРЕБОВАНИЯ К ЛИНЕЙНОСТИ УСИЛИТЕЛЕЙ
- СЛОЖНОСТЬ РЕАЛИЗАЦИИ МОДЕМОВ

АНАЛОГОВАЯ МОДУЛЯЦИИ

- АНАЛОГОВАЯ МОДУЛЯЦИЯ
  - АМПЛИТУДНАЯ МОДУЛЯЦИЯ
    - АМПЛИТУДНАЯ МОДУЛЯЦИЯ С ОДНОЙ БОКОВОЙ ПОЛОСОЙ
    - БАЛАНСНАЯ АМПЛИТУДНАЯ МОДУЛЯЦИЯ
    - КВАДРАТУРНАЯ МОДУЛЯЦИЯ
  - УГЛОВАЯ МОДУЛЯЦИЯ
    - ЧАСТОТНАЯ МОДУЛЯЦИЯ
    - ЛИНЕЙНАЯ ЧАСТОТНАЯ МОДУЛЯЦИЯ
    - ФАЗОВАЯ МОДУЛЯЦИЯ
    - СИГНАЛЬНО-КОДОВАЯ МОДУЛЯЦИЯ

БАЛАНСНАЯ АМПЛИТУДНАЯ МОДУЛЯЦИЯ



Амплитудная модуляция (АМ) сводится к изменению амплитуды сигнала несущей частоты в соответствии с передаваемым сообщением

АМПЛИТУДНАЯ МОДУЛЯЦИЯ

Достоинства АМ:

- простые конструкции РПУ.

Недостатки АМ:

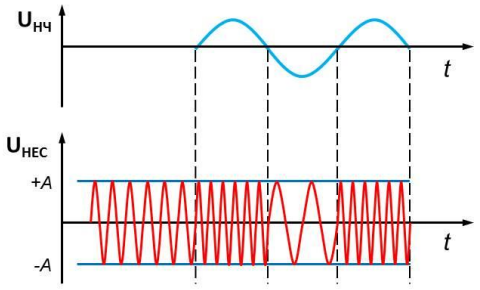
- низкая эффективность использования мощности передатчика,
- широкая полоса частот, вдвое превышающая ширину спектра модулирующего сигнала

Однополосная модуляция (ОМ) - является вариантом АМ с подавленной несущей и подавленной одной из боковых составляющих спектра.

Достоинства однополосной модуляции:

1. При однополосной модуляции мощность передатчика используется только для передачи полезного сигнала (сигнала, несущего информацию), за счет чего получить выигрыш в уровне сигнала как минимум в 4 раза.
2. За счет снижения полосы РПУ в два раза снижаются его шумы, т.е. ещё получается выигрыш в отношении сигнал/шум ещё в 2 раза.

УГЛОВАЯ МОДУЛЯЦИЯ



Частотная, фазовая модуляции (ЧМ, ФМ) – угловые методы модуляции.

В этом случае амплитуда сигнала неизменна, а частота и фаза изменяются в соответствии с передаваемым сообщением.

УГЛОВАЯ МОДУЛЯЦИЯ

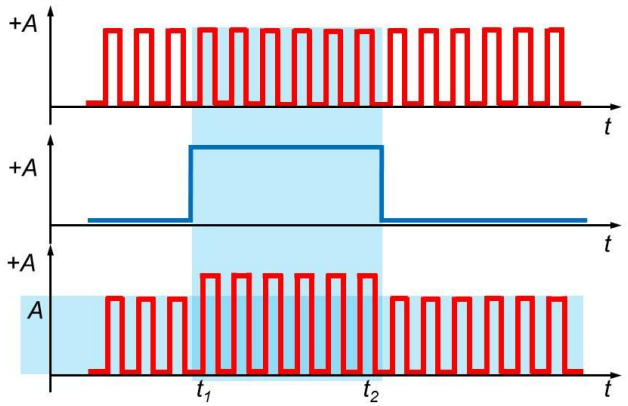
Достоинством ЧМ (ФМ) по сравнению с АМ:

- является более высокая помехоустойчивость угловых методов модуляции. Помехи, возникающие при распространении сигнала в атмосфере, приводят в основном к изменению амплитуды принимаемого сигнала, но не его частоты; поэтому при АМ помеховый сигнал добавляется к полезному сигналу, искажая его, чего нет при ЧМ, т.к. при нем в РПУ используется амплитудный ограничитель, что позволяет избавиться от паразитной АМ (помеховой АМ).
- Использование ЧМ и ФМ – эффективное средство борьбы с паразитной АМ и достоинством ЧМ является возможность применения амплитудных ограничителей.

ИМПУЛЬСНАЯ МОДУЛЯЦИЯ

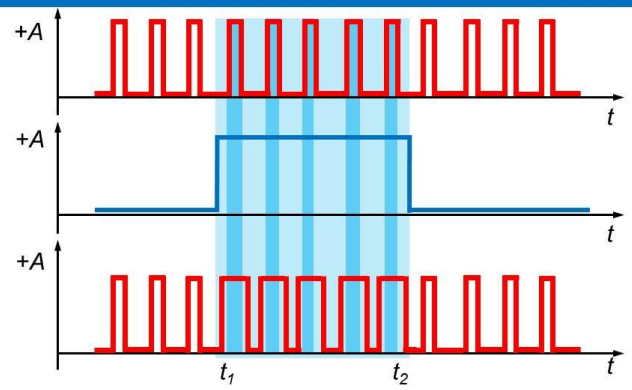
- **АМПЛИТУДНО ИМПУЛЬСНАЯ МОДУЛЯЦИЯ (АИМ)**
- **ШИРОТНО-ИМПУЛЬСНАЯ МОДУЛЯЦИЯ (ШИМ)**
- **ЧАСТОТНО-ИМПУЛЬСНАЯ МОДУЛЯЦИЯ (ЧИМ)**
- **ФАЗОВО-ИМПУЛЬСНАЯ МОДУЛЯЦИЯ (ФИМ)**

АМПЛИТУДНО - ИМПУЛЬСНАЯ МОДУЛЯЦИЯ



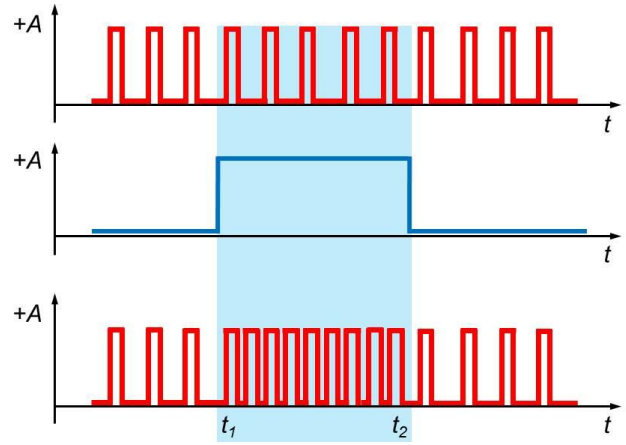
АИМ характеризуется низкой помехоустойчивостью.

ШИРОТНО - ИМПУЛЬСНАЯ МОДУЛЯЦИЯ

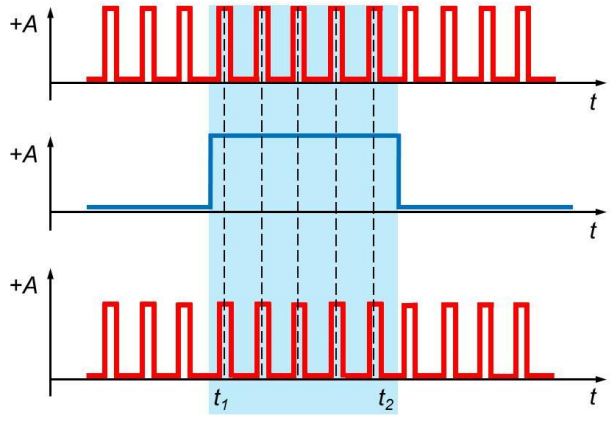


ШИМ более помехоустойчива, но широкая полоса РПУ, соответствующая минимальной τ_u, приводит к возрастанию шумов, таким образом к снижению помехоустойчивости.

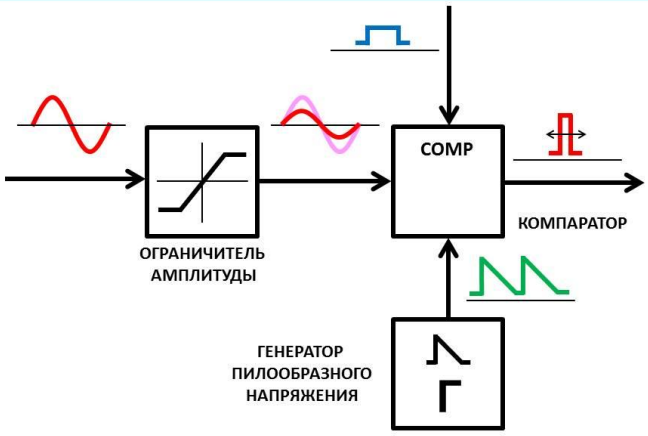
ЧАСТОТНО - ИМПУЛЬСНАЯ МОДУЛЯЦИЯ



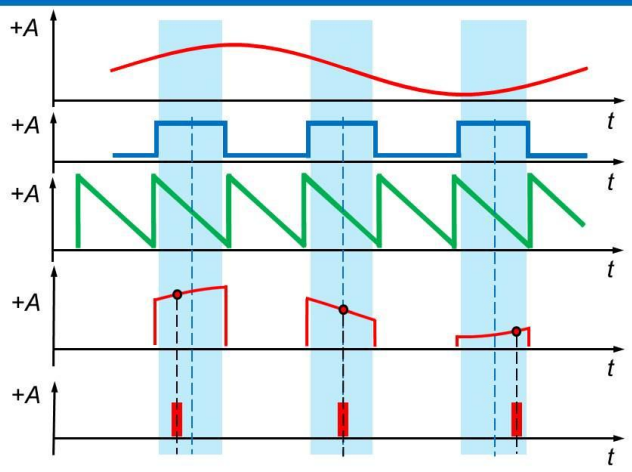
ФАЗОВО - ИМПУЛЬСНАЯ МОДУЛЯЦИЯ



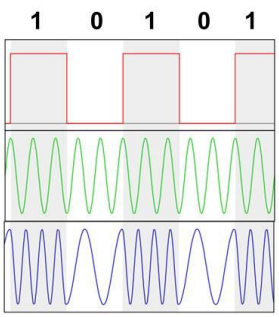
ФАЗОВО - ИМПУЛЬСНЫЙ МОДУЛЯТОР



ФАЗОВО - ИМПУЛЬСНАЯ МОДУЛЯЦИЯ



ЦИФРОВАЯ МОДУЛЯЦИЯ



Цифровая модуляция — процесс преобразования цифровых символов в сигналы, совместимые с характеристиками канала связи.

Каждому возможному значению передаваемого символа ставятся в соответствие некоторые параметры аналогового несущего колебания.

Манипуляция - способ цифровой модуляции, когда параметры несущего колебания меняются скачкообразно.

ЦИФРОВАЯ МОДУЛЯЦИЯ

При цифровой модуляции используют чаще всего дискретные последовательности двоичных символов — двоичных кодов.

Закодированный первичный аналоговый сигнал *e(t)*, представляющий собой последовательность кодовых символов $\{e_n\} = e_n^{(k)}$ (n = O, 1, 2, 3, ... — порядковый номер символа; к — номер позиции кода; m — основание кода, т. е. число различных его элементов, которые преобразуются в последовательность элементов (посылок) сигнала {Un(t)} путем воздействия кодовых символов на высокочастотное несущее колебание $U_H(t)$.

Как правило, используют двоичные коды т.е. m=2. Обычно посредством модуляции частота или фаза несущего в радиоимпульсе изменяется по закону, определяемому цифровым кодом.

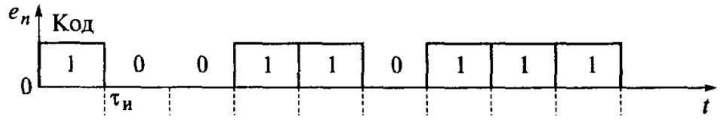
НЕ ВОЗВРАЩАЮЩИЙСЯ В НУЛЬ КОД – NRZ (Non Return to Zero)

Является простейшим линейным кодом, широко применяемым на практике.

Существуют две разновидности этого кода:

— **униполярный NRZ-код.**

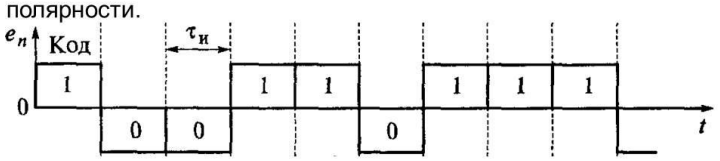
В униполярном NRZ-коде логической единице соответствует прямоугольный импульс положительной полярности, а логическому нулю — нулевое напряжение (пауза).



НЕ ВОЗВРАЩАЮЩИЙСЯ В НУЛЬ КОД – NRZ (Non Return to Zero)

— биполярный NRZ-код.

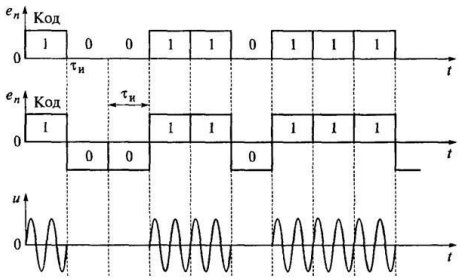
В биполярном NRZ-коде логической единице соответствует прямоугольный импульс положительной полярности, а логическому нулю — прямоугольный импульс отрицательной полярности.



Положительное или отрицательное напряжение на выходе кодера сохраняется неизменным в течение длительности символа, что и определяет термин «не возвращающийся в нуль» код. Длительность импульсов и пауз в NRZ-кодах равна длительности одного символа (бита) информации

АМПЛИТУДНАЯ МАНИПУЛЯЦИЯ

Амплитудная манипуляция (АМн; иначе ИКМ-АМ, или цифровая амплитудная модуляция — ЦАМ; amplitude shift keying — ASK).

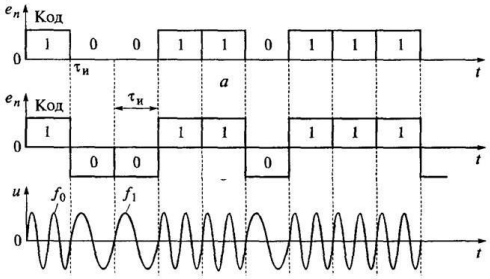


Битовому символу «1» при ИКМ-АМ соответствует передача несущего колебания в течение времени $\tau_И$ (длительность посылки), символу «0» — отсутствие колебания (пауза) на таком же временном интервале.

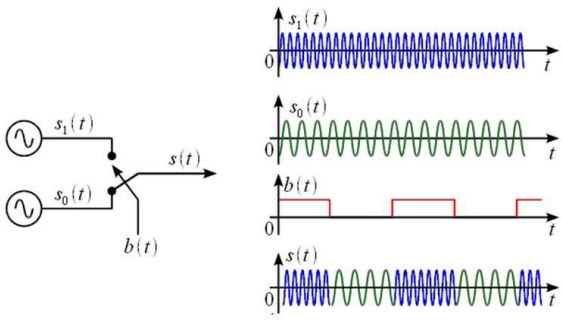
ЧАСТОТНАЯ МАНИПУЛЯЦИЯ

Частотная манипуляция (ЧМн; иначе ИКМ-ЧМ, или цифровая частотная модуляция — ЦЧМ; frequency shift keying — FSK).

При ИКМ-ЧМ передача несущего с частотой f_0 соответствует символу «1», а передача колебания с частотой f_1 — символу «0».



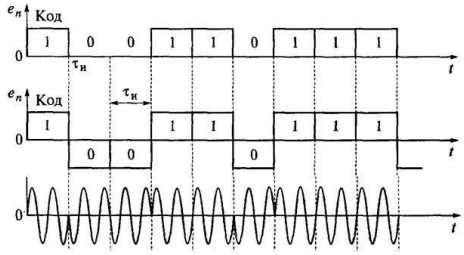
ПРИНЦИП ФОРМИРОВАНИЯ СИГНАЛА ЧАСТОТНОЙ МАНИПУЛЯЦИИ



ФАЗОВАЯ МАНИПУЛЯЦИЯ

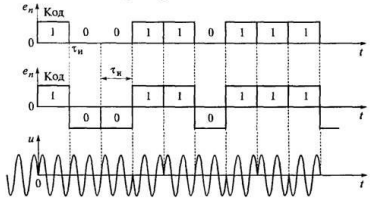
Фазовая манипуляция (ФМн; иначе ИКМ-ФМ, или цифровая фазовая модуляция — ЦФМ; phase shift keying — PSK).

При двоичной ИКМ-ФМ фаза несущей меняется на 180° при каждом переходе символов от «1» к «0» и от «0» к «1».



ОТНОСИТЕЛЬНАЯ ФАЗОВАЯ МАНИПУЛЯЦИЯ

Относительная фазовая манипуляция (ОФМ; differential phase shift keying — DPSK.

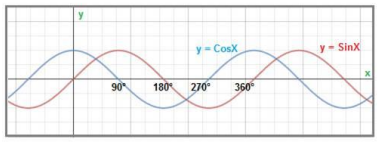


Изменение фазы несущего сигнала на 180^0 происходит при каждом «приходе» логической «1» - символ «0» передается отрезком синусоиды с начальной фазой предшествующего элемента сигнала, а символ «1» — таким же отрезком с начальной фазой, отличающейся от начальной фазы предшествующего элемента на 180°.

КВАДРАТУРНАЯ АМПЛИТУДНАЯ МАНИПУЛЯЦИЯ

При **квадратурной амплитудной модуляции** (QAM) передаваемый сигнал модулирует и амплитуду, и фазу несущего колебания. Это происходит одновременно и независимо.

Квадратурное представление сигналов является удобным и достаточно универсальным средством их описания. Заключается оно в представлении колебания линейной комбинацией из двух ортогональных составляющих - косинусоидальной и синусоидальной:



$$s(t) = a_k \cos \omega_0 t + b_k \sin \omega_0 t,$$

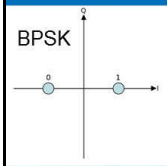
где a_k и b_k - биполярные дискретные величины

МНОГОПОЗИЦИОННЫЕ СИГНАЛЫ

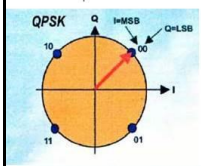
Для разных видов манипуляции существуют методы, позволяющие передавать не только 0 и 1 в рамках одного сигнала, такие методы получили название многопозиционные.

Суть этих методов в том, что один элемент линейного сигнала несет информацию о большем числе битов, чем в обычных двухпозиционных методах. Работает это очень просто. Например, в многопозиционной амплитудной манипуляции зададим не 2 амплитуды, которые будут кодировать 0 или 1, а 4, которые будут соответствовать 00, 01, 10, 11 по мере увеличения амплитуды. Для многопозиционной частотной манипуляции используется больше частот, а для многопозиционной фазовой манипуляции, соответственно, больше сдвигов. Да, это действительно позволяет повысить удельную скорость передачи информации, но при этом начинают возникать ошибки, связанные с погрешностью передачи.

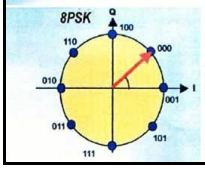
МНОГОПОЗИЦИОННЫЕ СИГНАЛЫ



Binary Phase Shift Keying является обычной бинарной фазовой манипуляцией, позволяет закодировать 1 бит информации за сигнал.



Quadrature Phase Shift Keying переводится как квадратурная фазовая манипуляция и представляет собой разделение на 4 фазы, которые позволяют закодировать 2 бита за сигнал.



8 Phase Shift Keying представляет собой разделение на 8 фаз, которые позволяют закодировать 3 бита за сигнал.

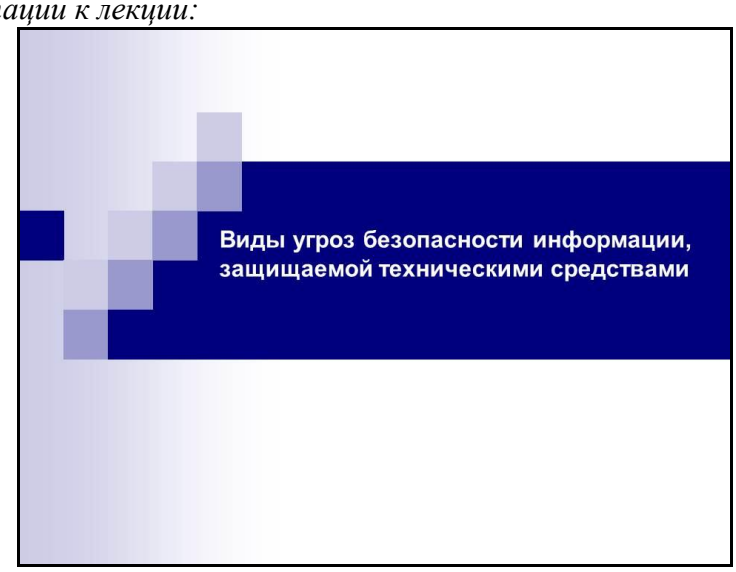
Литература: Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д. А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. URL: http://biblioclub.ru/index.php?page=book&id=429070

Лекция 5. Виды угроз безопасности информации, защищаемой техническими средствами

Тезисы лекции:

- Угрозы утечки информации.
- Угрозы преднамеренных воздействий.
- Угрозы случайных воздействий.
- Технические каналы утечки информации: наблюдение, подслушивание, перехват.
- Источники угроз безопасности информации.
- Опасные сигналы и их источники.

Слайды презентации к лекции:



Термины и определения.

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации в соответствии с заданной информационной технологией, а так же помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены.

Объекты информатизации, на которых обработка информации осуществляется с использованием средств вычислительной техники (СВТ), называют "**объектами СВТ**".

Защищаемый объект информатизации (объект защиты) – объект информатизации, предназначенный для обработки важной информации с обеспечением требуемого уровня ее защиты.

При рассмотрении объекта СВТ, как объекта защиты от утечки информации по техническим каналам, его необходимо рассматривать как объект, включающий в себя:

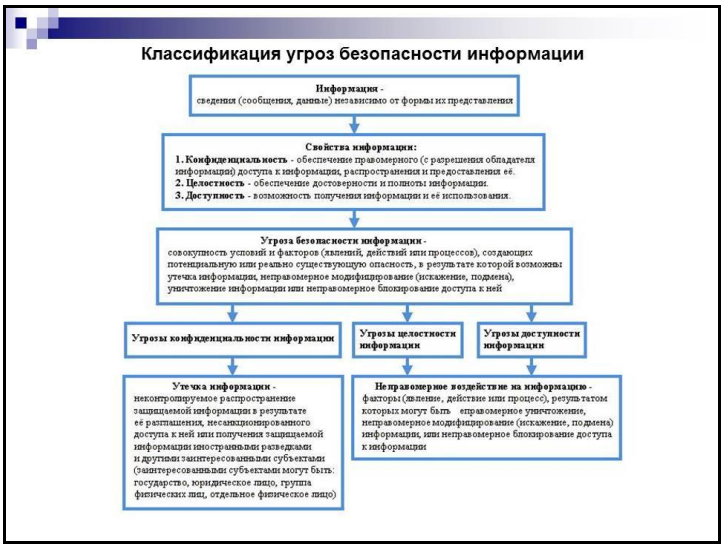
- технические средства и системы, непосредственно обрабатывающие информацию ограниченного доступа (**ТСОИ** - **ОТС**), вместе с их соединительными линиями (совокупность проводов и кабелей, прокладываемых между отдельными ТСОИ и их элементами);
- вспомогательные технические средства и системы (**ВТСС**) вместе с их соединительными линиями;
- посторонние проводники;
- систему электропитания;
- систему заземления.

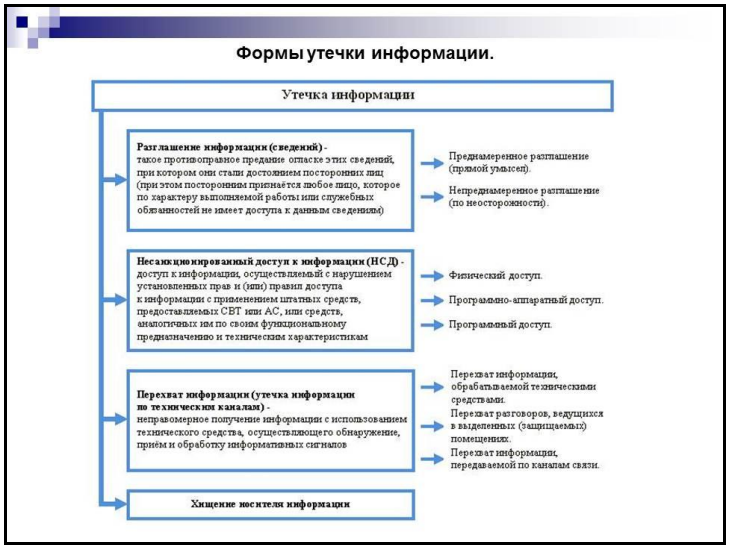
Безопасность информации – состояние защищенности информации, при котором с требуемым уровнем обеспечены ее конфиденциальность, целостность и доступность.

Угроза безопасности информации – потенциальная или реальная возможность нарушения безопасности информации, обрабатываемой с помощью технических средств.

Термины и определения.

- **Техническая разведка** – деятельность по получению важной (защищаемой) информации с помощью технических средств.
- **Средство технической разведки** – аппаратура технической разведки, размещенная на стационарном или мобильном объекте (помещении, транспортном средстве и т.д.), и обслуживаемая соответствующим персоналом.
- **Аппаратура технической разведки** – совокупность технических устройств, предназначенных для обнаружения, приема (перехвата), регистрации и обработки сигналов, содержащих важную (защищаемую) информацию.
- **Возможности технической разведки** – характеристики способности обнаружения, распознавания, приема и регистрации информативных сигналов (ПЭМИН) средствами технической разведки.
- **Зона разведдоступности** – пространство вокруг объекта, в пределах которого реализуются возможности технической разведки.
- **Модель технической разведки** – описание средств технической разведки, содержащее их технические характеристики и тактику применения в объеме, достаточном для оценки возможностей технической разведки.
- **Информативный (опасный) сигнал** – электрические или электромагнитные сигналы и поля, по параметрам которых может быть раскрыта информация, обрабатываемая с помощью технических средств.


Классификация угроз безопасности информации
Информация -
сведения (сообщения, данные) независимо от формы их представления
Свойства информации:
1. Конфиденциальность - обеспечение правомерного (с разрешения обладателя информации) доступа к информации, распространения и предоставления её.
2. Целостность - обеспечение достоверности и полноты информации.
3. Доступность - возможность получения информации и её использования.
Угроза безопасности информации -
совокупность условий и факторов (явлений, действий или процессов), создающих потенциальную или реально существующую опасность, в результате которой возможны утечка информации, неправомерное модифицирование (искажение, подмена), уничтожение информации или неправомерное блокирование доступа к ней
Угрозы конфиденциальности информации
Угрозы целостности информации
Угрозы доступности информации
Утечка информации -
неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к ней или получения защищаемой информации иностранными разведками и другими заинтересованными субъектами (заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо)
Неправомерное воздействие на информацию -
факторы (явление, действие или процесс), результатом которых могут быть неправомерное уничтожение, неправомерное модифицирование (искажение, подмена) информации, или неправомерное блокирование доступа к информации


Формы утечки информации.
Утечка информации
Разглашение информации (сведений) -
такое противоправное предание огласке этих сведений, при котором они стали достоянием посторонних лиц (при этом посторонним признаётся любое лицо, которое по характеру выполняемой работы или служебных обязанностей не имеет доступа к данным сведениям)
Преднамеренное разглашение (прямой умысел).
Непреднамеренное разглашение (по неосторожности).
Несанкционированный доступ к информации (НСД) -
доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации с применением штатных средств, предоставляемых СВТ или АС, или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам
Физический доступ.
Программно-аппаратный доступ.
Программный доступ.
Перехват информации (утечка информации по техническим каналам) -
неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов
Перехват информации, обрабатываемой техническими средствами.
Перехват разговоров, ведущихся в выделенных (защищаемых) помещениях.
Перехват информации, передаваемой по каналам связи.
Хищение носителя информации


Возможные варианты утечки информации, обрабатываемой СВТ.
Для информации, обрабатываемой СВТ, актуальны все ранее перечисленные формы утечки, например:
Разглашение информации: передача носителя информации постороннему лицу (преднамеренное) или обработка информации на СВТ в присутствии посторонних лиц (непреднамеренное).
НСД к информации: вскрытие системного блока СВТ и изъятие HDD диска для копирования (физический), сброс установленных параметров BIOS и изменение приоритета последовательности загрузки носителя с последующей загрузкой альтернативной операционной системы и копированием интересующей информации на flash-накопитель (программно-аппаратный), внедрение в СВТ вредоносных программ для осуществления НСД к информации или её копирования (программный).
Хищение носителей информации.
Утечка информации по техническим каналам.
ПЕРЕДАЧА ИНФОРМАЦИИ СПЕЦИАЛЬНЫМИ ЗАКЛАДКАМИ
НАВОДКА НА ЛИНИИ СВЯЗИ, КОММУНИКАЦИИ И АППАРАТУРУ
УТЕЧКИ ЗА СЧЕТ ПЭМИ
НСД К ВИНЧЕСТЕРУ
УТЕЧКИ ПО ЭЛЕКТРОМАГНИТНОМУ КАНАЛУ
ИЗЛУЧЕНИЕ ТЕРМИНАЛА
ПРОСМОТР ИЗОБРАЖЕНИЯ НА ЭКРАНЕ
УТЕЧКИ ПО СЕТИ ПИТАНИЯ
Сеть
УТЕЧКИ ПО ЦЕПЯМ ЗАЗЕМЛЕНИЯ
НЕСАНКЦИОНИРОВАННОЕ КОПИРОВАНИЕ ДИСКЕТ
УТЕЧКА ИНФОРМАЦИИ ПО АКУСТИЧЕСКОМУ КАНАЛУ
ПРЯМОЕ ХИЩЕНИЕ ИНФОРМАЦИИ НА НОСИТЕЛЯХ И ДОКУМЕНТАХ
УТЕЧКА С КЛАВИАТУРЫ
Модель каналов утечки информации и способов несанкционированного доступа ПЭВМ

Понятие технического канала утечки информации.

- **Под техническим каналом утечки информации (ТКУИ)** понимают совокупность объекта разведки, технического средства разведки (**ТСР - СТР**), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал.
- По сути, под **ТКУИ** понимают способ получения с помощью **ТСР** разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.
- Совокупность источника информативного сигнала (в данном случае - СВТ), технического средства осуществляющего перехват информации и физической среды, в которой распространяется информативный сигнал, называется ***техническим каналом утечки информации***.

В зависимости от природы образования информативного сигнала технические каналы утечки информации можно разделить на естественные и специально создаваемые:

- **Естественные каналы утечки информации** образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (***электромагнитные каналы утечки информации***), а также вследствие наводок информативных сигналов в линиях электропитания и заземления СВТ, соединительных линиях ВТСС и посторонних проводниках (***электрические каналы утечки информации***)
- К **специально создаваемым каналам утечки информации** относятся каналы, создаваемые путём внедрения в СВТ электронных устройств перехвата информации (закладных устройств) и путём “высокочастотного облучения” СВТ.

Определение СТС.

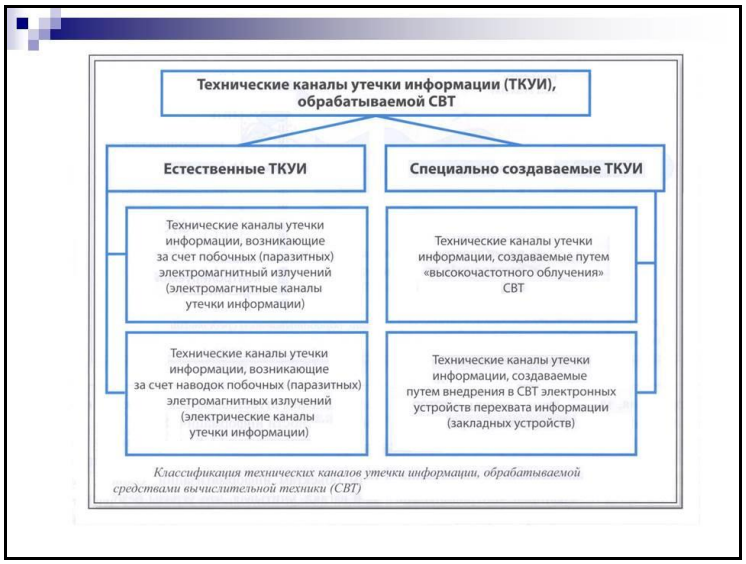
Постановлением Правительства РМ № 100 от 9 февраля 2009 г. дано определение специальным техническим средствам, предназначенным для негласного получения информации: технические и/или программные средства, разработанные, приспособленные или запрограммированные для съема, получения, перехвата, сбора, прослушивания, регистрации и передачи акустических, видовых, электромагнитных и других сигналов с целью получения негласного доступа к информации, в том числе циркулирующей в сетях электронных коммуникаций.

В соответствии с **Классификатором специальных технических средств, предназначенных для негласного получения информации** (Приложение № 2 к Постановлению Правительства РМ № 100 от 9 февраля 2009 г.) к СТС отнесены следующие технические средства:

- **п. 5** СТС для негласного перехвата и регистрации информации, циркулирующей в информационных системах и сетях передачи данных (Тарифная позиция Товарной номенклатуры Республики Молдова из 8471 49 000 и из 8517 69 900).
- **п. 6** СТС для получения несанкционированного доступа к информации, находящейся в информационных системах или на других технических средствах хранения информации (Тарифная позиция Товарной номенклатуры Республики Молдова из 8471 49 000).

СТС для негласного перехвата и регистрации информации, циркулирующей в информационных системах.





Классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники (СВТ)

Обобщенная структурная схема ТКУИ, обрабатываемой СВТ.

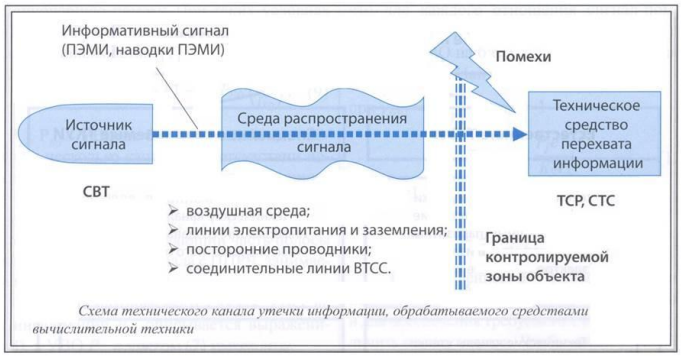


Схема технического канала утечки информации, обрабатываемого средствами вычислительной техники

Естественные ТКУИ: электромагнитный и электрический.

В **электромагнитных каналах утечки информации** носителем информации являются электромагнитные излучения (ЭМИ), возникающие при обработке информации техническими средствами.

Основными причинами возникновения электромагнитных каналов утечки информации в ТСОИ являются:

- побочные электромагнитные излучения, возникающие вследствие протекания информативных сигналов по элементам ТСОИ;
- модуляция информативным сигналом побочных электромагнитных излучений высокочастотных генераторов ТСОИ;
- модуляция информативным сигналом паразитного электромагнитного излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты).

Причинами возникновения **электрических каналов утечки информации** являются наводки информативных сигналов (под которыми понимаются токи и напряжения в токопроводящих элементах), вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

Наводки информативных сигналов могут возникнуть:

- в линиях электропитания ТСОИ;
- в линиях электропитания и соединительных линиях ВТСС;
- в цепях заземления ТСОИ и ВТСС;
- в посторонних проводниках (металлических трубах систем отопления, водоснабжения, металлоконструкциях и т.д.).

Понятие ПЭМИ.

- **Побочные электромагнитные излучения (ПЭМИ)** – нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации.

  С точки зрения защиты информации опасность представляют информативные ПЭМИ, содержащие в себе признаки обрабатываемой информации.
- **Информативными ПЭМИ** называются сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением выводимым на монитор, данными обрабатываемыми на устройствах ввода-вывода и т.д.).
- **Неинформативными ПЭМИ** называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ.

- ПЭМИ возникают при различных режимах обработки информации средствами вычислительной техники:
  - вывод информации на монитор;
  - ввод данных с клавиатуры;
  - запись информации на накопители;
  - чтение информации с накопителей;
  - передача данных в каналы связи;
  - вывод данных на печатные устройства;
  - запись данных от сканера и т.д.

  При каждом режиме работы СВТ возникают ПЭМИ, имеющие свои характерные особенности.

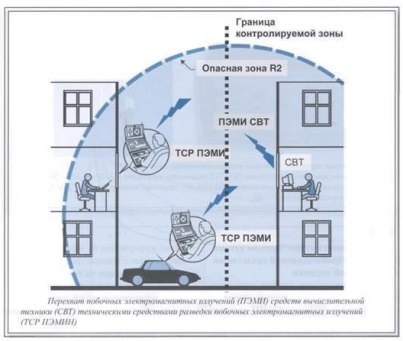
  Диапазон возможных частот ПЭМИ зависит от типа СВТ и может составлять от сотен Гц до десятков ГГц.

Основными источниками возникновения ПЭМИ при работе СВТ являются:

- Процессор, шина данных процессора и цепи питания.
- Контроллеры и мост чипсета.
- Модули памяти и шина данных.
- Инверторы питания перечисленных выше устройств.
- HDD и шины IDE (ATA) и SATA.
- CD и шина IDE (ATA).
- Видеокарта и шина AGP или E-PCI.
- COM порт и внешние подключения по нему.
- LTP порт и внешние подключения по нему.
- USB порт.
- VGA и другие виды портов, предназначенные для подключения мониторов.
- Беспроводные сетевые адаптеры IEEE 802 для локальных сетей.



Принцип перехвата ПЭМИ СВТ.



- **Зона 2** (***R2***) – пространство вокруг технического средства обработки информации (объекта), в пределах которого возможен перехват побочных электромагнитных излучений и последующее восстановление содержащейся в них информации.
- В **зоне 2** отношение “сигнал/помеха” для составляющих электромагнитного поля опасного сигнала превышает допустимое нормированное значение.

Структурная схема электромагнитного ТКУИ, обрабатываемой СВТ.

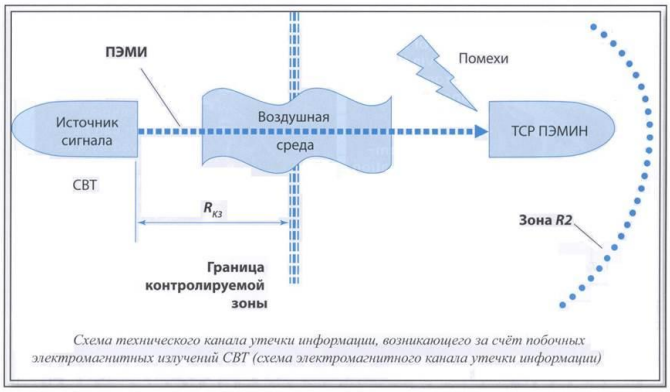


Схема технического канала утечки информации, возникающего за счёт побочных электромагнитных излучений СВТ (схема электромагнитного канала утечки информации)

Образцы оборудования для перехвата ПЭМИ.



а) б)

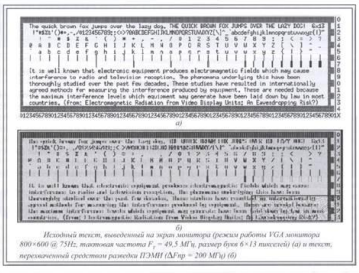
Комплекс перехвата побочных электромагнитных излучений СВТ:
а) специальное приёмное устройство PKI 2715 (дальность перехвата ПЭМИ от 10 до 50 м);
б) широкополосная направленная антенна R&S HL 007 (диапазон частот от 80 МГц до 1,3 ГГц, коэффициент усиления 5-7 дБ)

Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.



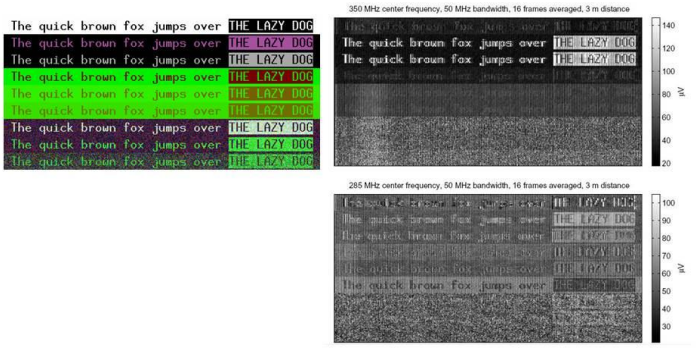
а) б)

Тестовое изображение, выведенное на экран монитора (а) и изображение, перехваченное средствами разведки ПЭМИ (б)

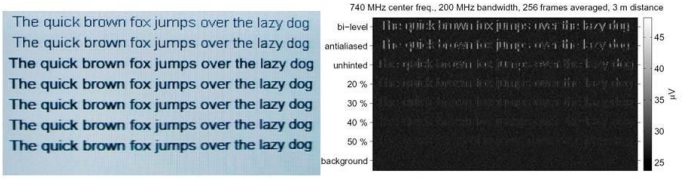


Исходный текст, выведенный на экран монитора (режим работы VGA монитора 800×600 @ 75Hz, тактовая частота $F_т$ = 49,5 МГц, размер букв 6×13 пикселей) (а) и текст, перехваченный средствами разведки ПЭМИ (ΔFпр = 200 МГц) (б)

Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.

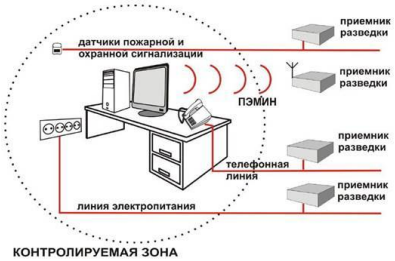


Образцы изображений, полученных с помощью перехвата ПЭМИ СВТ.



В зависимости от выбранных параметров шрифта (тип шрифта, размер букв, цвет текста и т.д.) качество перехватываемого за счёт ПЭМИ изображения будет различным.

Понятие ПЭМИН.



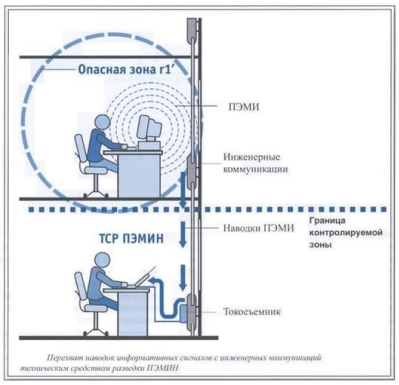
Электромагнитная наводка – передача (индуцирование) электрических сигналов из одного устройства (цепи) в другое, непредусмотренная схемными или конструктивными решениями и возникающая за счет паразитных электромагнитных связей.
Электромагнитные наводки могут приводить к утечке информации по токопроводящим коммуникациям, имеющим выход за пределы контролируемой зоны.

Причинами возникновения электрических каналов утечки информации являются наводки информативных сигналов, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить на:

- наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИ ТСОИ;
- наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и индуктивными связями ("просачивание" информативных сигналов в цепи электропитания через блоки питания ТСОИ);
- наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ.

Принцип перехвата ПЭМИН СВТ.



Перехват наводок информативных сигналов с инженерных коммуникаций техническим средством разведки ПЭМИН

- **Зона 1** (***r1***)– пространство вокруг технического средства обработки информации (объекта), в пределах которого на случайных антеннах может наводиться опасный (информативный) сигнал выше допустимого (нормированного) уровня.
- В **зоне 1** запрещается размещение случайных антенн, через которые может происходить утечка важной информации за пределы контролируемой зоны.
- **Случайная антенна –** электрические и коммуникационные цепи вспомогательных технических средств и систем, а так же сами ВТСС, способные принимать побочные электромагнитные излучения.

  Случайные антенны могут быть сосредоточенными и распределенными.

Структурная схема электрического ТКУИ, обрабатываемой СВТ.

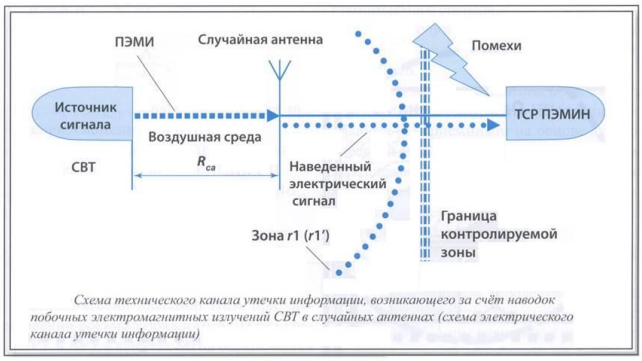
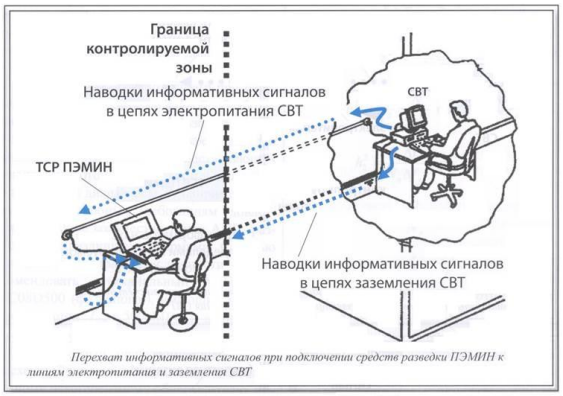


Схема технического канала утечки информации, возникающего за счёт наводок побочных электромагнитных излучений СВТ в случайных антеннах (схема электрического канала утечки информации)

Уровень наводок зависит от расстояния между источником излучения и случайной антенной, типа случайной антенны (сосредоточенная или распределённая), длиной параллельного пробега и величиной переходного затухания линий, напряжения информативного сигнала в линии и уровня шумов (помех) и других факторов.

Принцип перехвата ПЭМИН СВТ по цепям электропитания и заземления.



Перехват информативных сигналов при подключении средств разведки ПЭМИН к линиям электропитания и заземления СВТ

Структурная схема перехвата ПЭМИН СВТ по цепям электропитания.

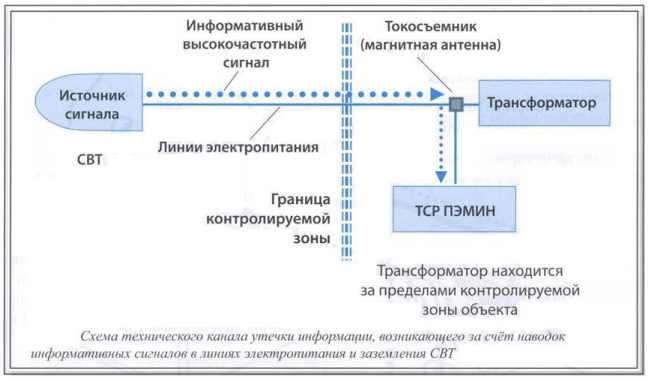


Схема технического канала утечки информации, возникающего за счёт наводок информативных сигналов в линиях электропитания и заземления СВТ

Структурная схема перехвата ПЭМИН СВТ по цепям заземления.

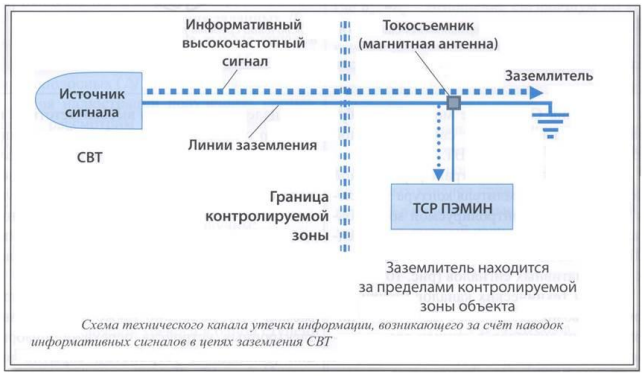
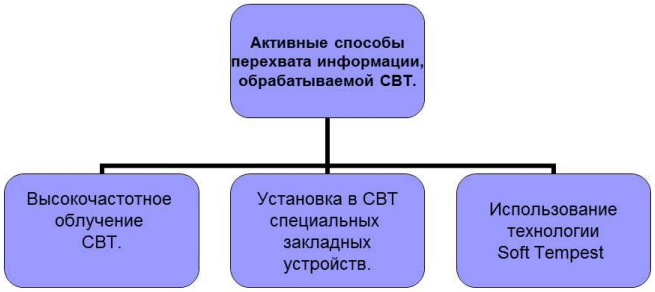
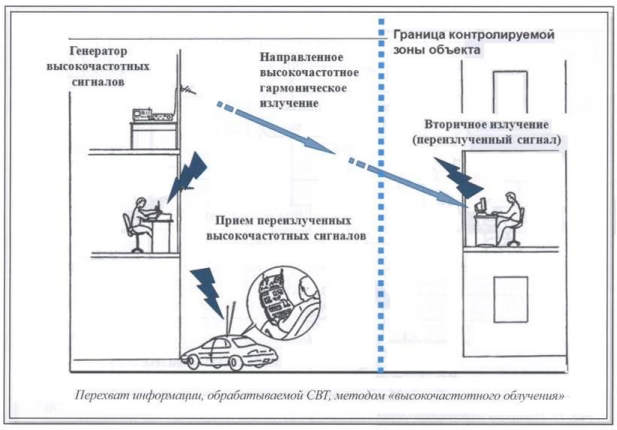


Схема технического канала утечки информации, возникающего за счёт наводок информативных сигналов в цепях заземления СВТ

Специально создаваемые ТКУИ, обрабатываемой СВТ.



Принцип перехвата информации, обрабатываемой СВТ, методом "высокочастотного облучения".



Перехват информации, обрабатываемой СВТ, методом «высокочастотного облучения»

Структурная схема ТКУИ, создаваемого методом "высокочастотного облучения" СВТ.

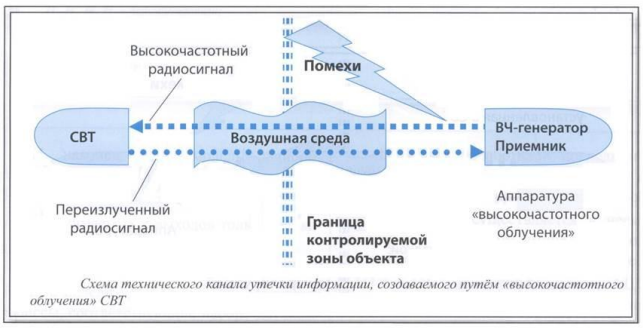


Схема технического канала утечки информации, создаваемого путём «высокочастотного облучения» СВТ

СВТ облучается мощным высокочастотным гармоническим сигналом (используется ВЧ-генератор с направленной антенной, имеющей узкую диаграмму направленности).
При взаимодействии облучающего электромагнитного поля с элементами СВТ происходит модуляция вторичного излучения информативным сигналом. Переизлучённый сигнал принимается приёмным устройством ТСР и детектируется.

Специальные закладные устройства, устанавливаемые в СВТ.

Под **аппаратной закладкой** понимают электронное устройство, скрытно устанавливаемое (внедряемое) в СВТ с целью обеспечить утечку информации, нарушение ее целостности или блокирование.

Аппаратная закладка, как правило, состоит из:

- блока перехвата;
- блока передачи информации (или модуля записи информации);
- блока ДУ (при необходимости);
- блока питания.

Блок перехвата подключается к информационным кабелям или к платам блоков СВТ и осуществляет перехват информационных сигналов, их обработку и преобразование в вид, удобный для записи или передачи на приемный пункт.

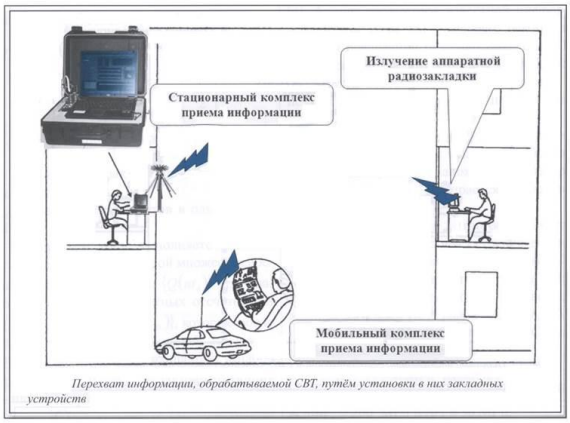
Перехватываемая аппаратными закладками информация может записываться в память ЗУ (например, на flash-память) или передаваться на приемный пункт по радиоканалу, электросети, выделенной линии, оптическому каналу (при использовании ИК-порта) и т.п.

С помощью системы ДУ осуществляется включение/выключение устройства (запуск программы перехвата информации), включение/выключение режима передачи информации, установка параметров процесса съема и передачи информации.

Классификация закладных устройств, устанавливаемых в СВТ.

Показатель классификации	Значения
Вид перехватываемой информации	1. Видеоизображение, выводимое на экран монитора. 2. Информация, вводимая с клавиатуры. 3. Информация, выводимая на принтер. 4. Информация, записываемая на жесткий диск компьютера (HDD). 5. Информация, записываемая на внешние накопители (flash-память, CD, DVD, USB-накопители). 6. Информация, передаваемая по каналу связи.
Место установки	1. В корпусе системного блока. 2. Подключаемые к внешним разъемам системного блока (например, USB). 3. Подключаемые в виде переходных элементов в разрыв информационных кабелей, соединяющих системный блок с оконечными устройствами, например, клавиатурой, принтером и т.п. 4. В корпусе монитора. 5. В корпусе клавиатуры. 6. В корпусе принтера. 7. В корпусе модема и т.п.
Способ передачи информации	1. Без передачи информации (перехваченная информация записывается на специальные цифровые накопители, например, на flash-память). 2. По радиоканалу. 3. По сети 220 В. 4. По выделенной линии. 5. По оптическому каналу.
Средство передачи информации	1. Специальное радиопередающее устройство. 2. ИК-порт. 3. Устройства типа Bluetooth. 4. Устройства типа Wi-Fi, WiMAX и т.д.
Тип источника питания	1. От низковольтных источников питания технических средств. 2. От сети 220 В.
Вид исполнения	1. Обычные (отдельные модули). 2. Камуфлированные под типовые элементы электронных устройств.
Способ управления передатчика	1. Неуправляемые (с включением передатчика при включении СВТ). 2. Дистанционно управляемые.
Способ накопления информации	1. Без накопления. 2. С промежуточным накоплением (с коротким и длительным временем накопления).
Способ кодирования информации	1. Без кодирования информации. 2. С цифровым шифрованием информации.

Принцип перехвата информации, обрабатываемой СВТ, с помощью установки в них специальных закладных устройств.



Перехват информации, обрабатываемой СВТ, путём установки в них закладных устройств

Структурная схема ТКУИ, создаваемого путём установки в СВТ специальных закладных устройств.

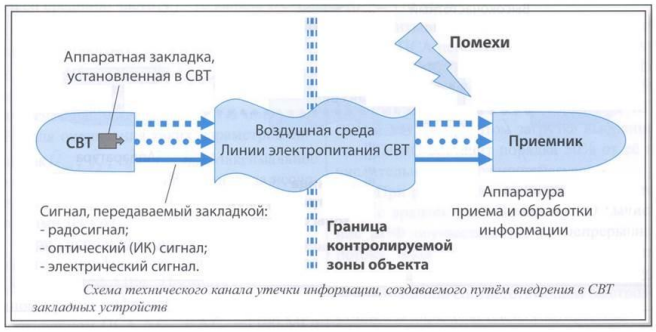


Схема технического канала утечки информации, создаваемого путём внедрения в СВТ закладных устройств

Аппаратные закладки для перехвата информации, вводимой с клавиатуры ПЭВМ (аппаратные кейлоггеры).

Аппаратные кейлоггеры (***keylogger hardware***) являются самыми распространёнными закладными устройствами и предназначены в основном для перехвата паролей пользователей и текстовых документов, набираемых с использованием ПЭВМ.

Данные устройства могут подключаться в разъем между системным блоком и клавиатурой (изготавливаются в виде переходников или удлинительных кабелей), а так же скрытно устанавливаться в корпусе клавиатуры или внутри системного блока с подключением к интерфейсу клавиатуры.

Перехватываемая информация может передаваться на контрольный пункт в режиме реального времени по радиоканалу или записываться на flash-память.

Существуют модели кейлоггеров с накоплением, которые по внешней команде передают записанную информацию по радиоканалу (в том числе, используя технологию Wi-Fi).





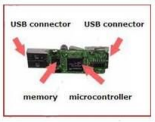
Принцип работы аппаратного кейлоггера с записью информации на flash-память, устанавливаемого в разъем между клавиатурой и системным блоком ПЭВМ.

Аппаратные кейлоггеры с записью информации на flash-память состоят из датчика, осуществляющего перехват сигналов, передаваемых от клавиатуры в системный блок, микроконтроллера и модуля памяти.

Такие кейлоггеры не требуют дополнительного питания и работают под управлением любой ОС.

Кейлоггер записывает все нажатия клавиш в собственную память, в специальный файл (обычно формата ".txt"). После того, как память кейлоггера заполнится, он прекращает запись информации.

Встроенная память на 2Гб позволяет осуществлять непрерывную запись информации в течение полутора лет без ее очистки.





Варианты аппаратных кейлоггеров, устанавливаемых между клавиатурой и системным блоком ПЭВМ.

В зависимости от конкретной модели кейлоггер имеет следующие основные характеристики:

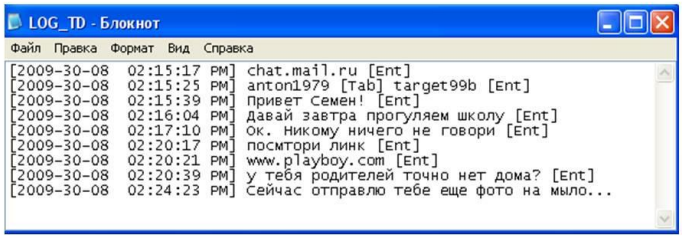
- Запись информации осуществляется на flash-память объёмом от 64 Кб до 2 ГГб. Объём памяти 1 МГб обеспечивает запись до 2000000 нажатий клавиш или 500 страниц текста.
- Защита памяти 128 битной системой шифрования данных.
- Возможность записи и чтения текста на различных языках.
- Возможность установки модуля, позволяющего фиксировать время и дату набранного на клавиатуре текста с точностью до секунды.
- Совместимость со всеми проводными клавиатурами соответствующего типа (PS/2 или USB).
- "Невидимость" для операционной системы, невозможность обнаружения с помощью антивирусных программ.







Пример файла-отчёта аппаратного кейлоггера с записью информации на flash-память.



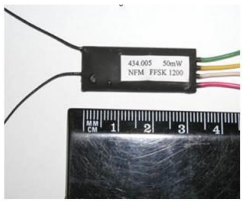
Принцип работы аппаратного кейлоггера с передачей информации по радиоканалу, устанавливаемого в разъем между клавиатурой и системным блоком ПЭВМ.



- Аппаратный кейлоггер - это чисто электронное устройство, которое не требует установки какого-либо дополнительного ПО, вмешательства в ОС, драйверы и т.п. Однако, у большинства аппаратных кейлоггеров есть недостаток - периодически требуется физический доступ к компьютеру для "переброса" информации из памяти кейлоггера. Этого недостатка нет у так называемых "радиокейлоггеров" (Wireless Keylogger).
- Радио (или беспроводной) кейлоггер состоит из двух основных модулей: передатчика и приемника. Передатчик и приемник сделаны под PS/2 и USB удлинители с т.н. "балуном" (ферритовое кольцо - фильтр). Сам модуль кейлоггера находится в передатчике, который является PS/2 аппаратным кейлоггером с встроенным радиопередающим модулем на 2.4 ГГц. Все нажатия клавиш клавиатуры передаются в реальном времени по радиоканалу. Приемник подключен через USB-порт к другому компьютеру, на котором с помощью специального ПО отображаются принятые данные.
- Вся система работает в режиме реального времени: текст, который набирается на клавиатуре с передатчиком, сразу же виден на приемной стороне. Максимальный радиус действия составляет около 50 метров. В здании с 3-4 стенами радиус действия составляет около 20 метров (зависит от толщины стен).

Принцип работы аппаратного кейлоггера с передачей информации по радиоканалу, скрытно устанавливаемого в клавиатуру ПЭВМ.





Кейлоггер **KS-1** - Keyboard Transmitter:

- Предназначен для перехвата информации, набираемой на клавиатуре типа PS/2.
- Устанавливается в клавиатуру ПК и передает информацию о нажатых клавишах по радиоканалу в цифровом виде (FFSK).
- Рабочая частота находится в диапазоне 430 МГц. Мощность передатчика 50 мВт, что обеспечивает дальность передачи на несколько сотен метров.
- Комплект состоит из самого кейлоггера **KS-1** и приемного оборудования (специальный приёмник, модем и ПО).
- Не обнаруживается антивирусными программами.

Аппаратные закладки для перехвата информации, выводимой на монитор ПЭВМ (аппаратные видеологгеры).



Видеологгер - это аппаратная закладка миниатюрных размеров, установленная в обычный видео кабель, соединяющий системный блок ПК с монитором.

Данное устройство подключается к **DVI, VGA** или **HDMI** порту компьютера и незаметно делает снимки экрана с заданной периодичностью, сохраняя их на встроенную flash-память в формате JPEG.

Для просмотра собранных скриншотов видеологгер подключается к USB порту через специальный USB ключ (входит в комплект). После этого устройство определится как новый съемный диск, на котором находится папка со снимками экрана в формате JPEG. Снимки содержат информацию о дате и времени сделанных скриншотов.

Основные характеристики типового аппаратного видеологгера.

- Совместим с разъемами **DVI, HDMI, VGA**.
- Поддерживает разрешение до Full-HD (1920 x 1080), а также WUXGA (1920 x 1200).
- Совместим со стационарными ПК и внешними мониторами, подключенными к ноутбукам.
- Не требует дополнительного питания (питается через USB шнур от USB порта).
- Встроенный JPEG кодировщик .
- 2 Гб встроенной памяти.
- Имеет встроенный модуль даты и времени с независимым источником питания (гарантийный срок службы 7 лет).
- Не требует установки драйверов, совместим с Winows, Linux и Mac OS.
- Имеет небольшие размеры и высокий уровень камуфляжа - выглядит как внешний мини кабель для монитора.
- Не обнаруживается антивирусными программами.



Аппаратно-программная закладка для отбора и копирования нужных файлов с ПК.





MAKE SECRET COPIES OF FILES AND DOCUMENTS FROM A PC, WHILE LEAVING NO TRACE

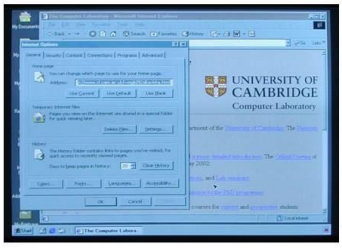
It scans a PC, and extracts the desired files and documents, in a matter of seconds!

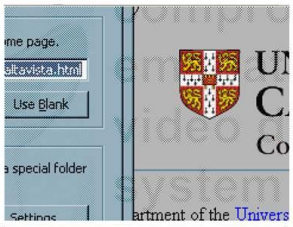
- To put your hands on files and documents without leaving any trace, our device is the absolute best choice!
  Do you need to quickly extract sensitive documentation and data files, while leaving no visible sign?
- For this purpose we have created a data extraction device, powerful and professional, and compatible with any Microsoft operating system, which can autonomously run on basically any hardware. Its quick setup and easy commands make it suitable for being used even by the less experienced of users.
- Our powerful data extractor is always ready to be used. Its operation is very simple: By connecting it to the victim's PC, all you have to do is activate it, and in a few seconds its intuitive graphic interface allows you to choose the file formats and types you wish to extract.
- Just click on OK and the graphic interface would then disappear while the device starts to operate in discreet mode.
  A few minutes is all it takes to analyze the PC hard drive and any external drives, USB sticks, network folders, CDs or DVDs. The device would silently extract sensitive information, files, documents, emails, images, folders and so on. Like a powerful magnet, it attracts the desired information, that you will later be able to view and analyze in depth.
- It contains no trojan or malware that could be blocked by an antivirus software, as the data extraction is done discreetly and without any trace left, just thanks to its high technological level.
- What would happen if our victim suddenly returns to their computer? No problem at all, thanks to our extractor the operation can be interrupted at any time, with no error message, alert or confirmation request; everything that has been captured up to that time would remain stored in the data extraction device.
- Our data extraction device can be concealed within a 16 GB USB drive or stick, with a fast and ground-breaking 2.0 firmware. This device can extract data at the whopping speed of 480 MB/s and is the most common of its kind, in terms of ease of use and operating speed, with a 100% success ratio. Designed specifically for this task, it can perfectly be adapted to any PC, making it very easy to retrieve the information you are looking for.

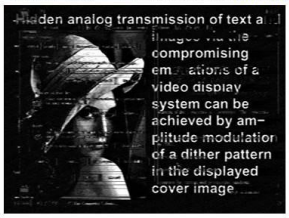
Использование технологии Soft Tempest для получения информации, обрабатываемой СВТ.

- Технология **Soft Tempest** – это технология скрытой передачи данных по каналу побочных электромагнитных излучений с помощью специальных программных средств. Данная технология заключается в том, чтобы целенаправленно управлять излучением компьютера с помощью специальных программных закладок.
- Технология **Soft Tempest** является разновидностью компьютерной стеганографии, т.е. метода скрытной передачи нужного (информативного) сообщения в обычных видео, аудио, графических и текстовых файлах ("файлах-контейнерах").
- Принцип реализации данной технологии следующий: нужный компьютер "заражается" специальной "программой-закладкой", а затем данная программа ищет необходимую информацию на диске и путем обращения к различным устройствам компьютера вызывает появление побочных излучений, содержащих нужный информативный сигнал. Например, учеными из Кембриджа была разработана "программа-закладка", которая "встраивала" информативное сообщение в композитный сигнал монитора. При этом были подобраны такие характеристики управляющих сигналов, что информация, излучаемая в эфир, отличалась от отображаемой на экране монитора.
- Если в качестве изображения, играющего роль стегоконтейнера, выбрать "обои" рабочего стола, то такое изображение не вызывает подозрений у пользователя компьютера, несмотря на то, что в это время в эфир излучается найденная "программой-закладкой" информация. Хотя методы Soft Tempest атаки, предложенные учеными Кембриджа, имели ряд недостатков – для передачи полезного сигнала используется сигнал монитора, что требует выполнения определенных условий (оператор должен использовать "нужную" экранную заставку, передача возможна при перерывах в работе оператора и т.д.) – они наглядно продемонстрировали реальность данного канала утечки информации.

Образцы изображений, полученных с помощью перехвата ПЭМИ, возникающих при использовании технологии Soft Tempest .







Восстановление изображения на мониторе ПК с помощью приёма переотражённого светового излучения монитора.

Одним из реальных каналов утечки информации, обрабатываемой на ПК, является визуальное наблюдение за экраном монитора.

Монитор ПК должен быть размещён таким образом, чтобы информация на его экране была недоступна для просмотра посторонними лицами.

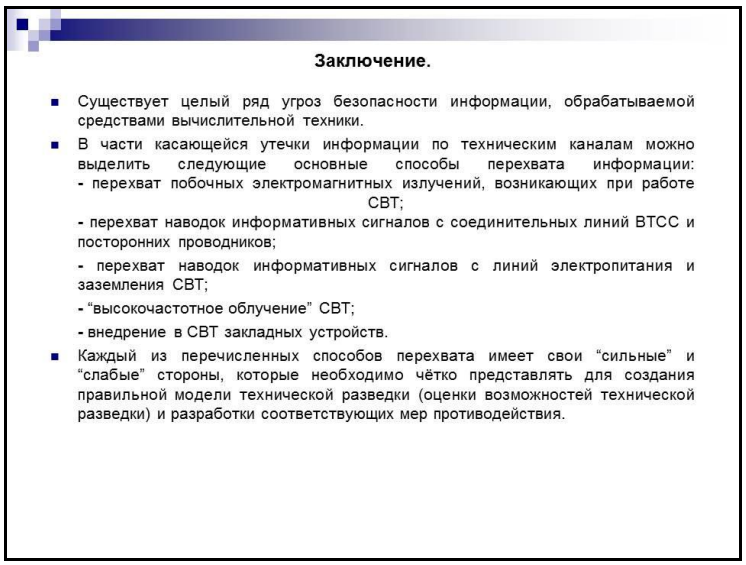
Однако световой поток от экрана монитора отражается от стен, и этот отраженный световой поток тоже может быть перехвачен.

В различных источниках (*см. список литературы*) было заявлено об успешных экспериментах по восстановлению изображения, принятого после его многократных отражений от стен и других окружающих предметов – *хотя лично для меня это непонятное "явление" как такое может быть.*



The Hamamatsu H6780-01 photosensor module used for these experiments contains a photomultiplier tube together with a high-voltage power supply.





Литература: Громов, Ю. Ю. Организация безопасной работы информационных систем [Электронный ресурс] : учеб. пособие для студентов / Ю. Ю. Громов. - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2014. - 132 с. URL: http://biblioclub.ru/index.php?page=book&id=277794

Лекция 6. Принципы добывания и обработки информации техническими средствами
Тезисы лекции:

- Способы и средства наблюдения в оптическом диапазоне. Обработка информации в оптическом приемнике.
- Способы и средства наблюдения в радиодиапазоне.
- Способы и средства перехвата сигналов.
- Обработка информации в радиоприемнике.
- Способы и средства подслушивания.
- Обработка информации в акустическом приемнике.

Материалы к лекции:



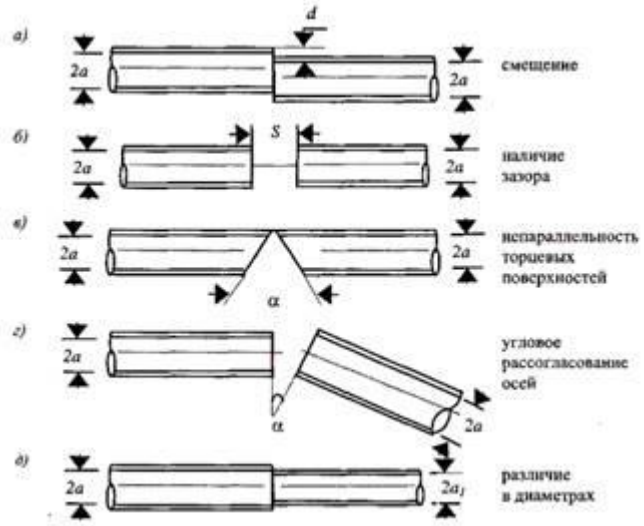
Объект наблюдения излучает и отражает свет другого источника как в видимом, так и ИК-диапазонах.

Длина (протяженность) канала утечки зависит от мощности света, от объекта, свойств среды распространения и чувствительности фотоприемника. Среда распространения в оптическом канале утечки информации возможна трех видов:

– безвоздушное (космическое) пространство;
– атмосфера;
– оптические световоды.

Таблица 3.2. Типовые варианты оптических каналов утечки информации

Объект наблюдения	Среда распространения	Оптический приемник
Документ, продукция в помещении	Воздух Воздух + стекло окна	Глаза человека + бинокль, фотоаппарат
Продукция во дворе, на машине, ж/платформе	Воздух Атмосфера + безвоздушное пространство	То же Фото, ИК, телевизионная аппаратура на КА
Человек в помещении, во дворе, на улице	Воздух Воздух + стекло	Глаза человека + бинокль, фото, кино, телевизионная аппаратура



Основными причинами излучения световой энергии в окружающее пространство в местах соединения оптических волокон являются:

– смещение (осевое несовмещение) стыкуемых волокон (рис. а);
– наличие зазора между торцами стыкуемых волокон (рис. б);
– непараллельность торцевых поверхностей стыкуемых волокон (рис. в);

– угловое рассогласование осей стыкуемых волокон (рис. г);
– различие в диаметрах стыкуемых волокон (рис. д).
Съем информации может быть осуществлен при принудительном (внешнем) изменении соотношения между показателями преломления сердцевины и оболочки за счет линейного электрооптического, фотоупругого и квадратичного электрооптического эффектов.

В оптическом (видимом и инфракрасном) диапазоне информация разведкой добывается путем визуального, визуально-оптического, фото- и киносъемки, телевизионного наблюдения, наблюдения с использованием приборов ночного видения и тепловизоров.
Эффективность обнаружения и распознавания объектов наблюдения зависит от следующих факторов :
– яркости объекта;
– контраста объект/фон;
– угловых размеров объекта;
– угловых размеров поля обзора;
– времени наблюдения объекта;
– скорости движения объекта.
При поиске объекта его форма не играет большой роли, а имеет значение только его площадь в пределах соотношения сторон от 1:1 до 1:10.
Увеличение угловых размеров объекта в 2 раза сокращает время, необходимое для его обнаружения, в 8 раз.

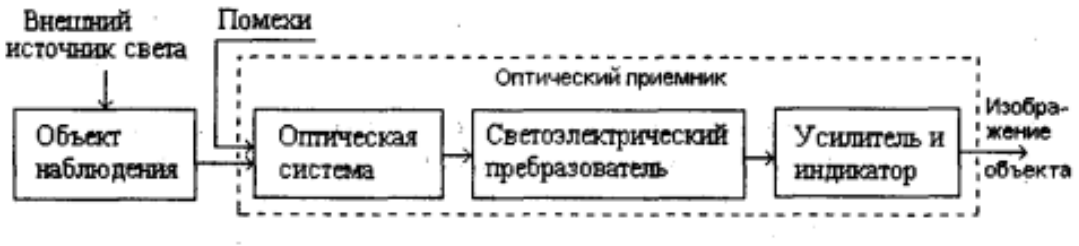


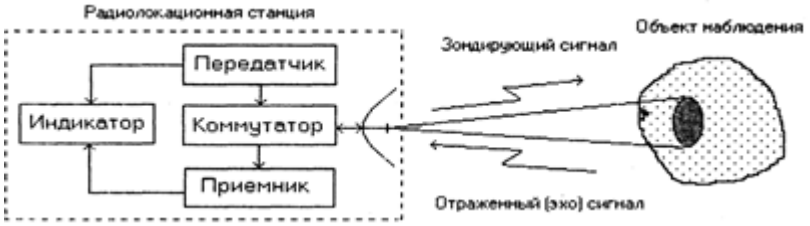
Рис. Структурная схема средства наблюдения в оптическом диапазоне

Оптическая система или объектив проецирует световой поток от объекта наблюдения на экран светоэлектрического преобразователя (сетчатку глаза, фотопленку, фотокатод, мишень оптико-электронного преобразователя). На мишени оптическое изображение преобразуется в электронное изображение, количество «свободных» электронов каждой точки которого пропорционально яркости соответствующей точки оптического изображения. Способы визуализации изображения для разных типов оптического приемника могут существенно отличаться. Изображение в виде зрительного образа формируется в мозгу человека, на фотопленке – в результате химической обработки светочувствительного слоя, на экране технического средства – путем параллельного или последовательного съема электронов с мишени, усиления электрических сигналов и формирования под их действием видимого изображения на экране с люминофором.

Радиолокационное и радиотеплолокационное наблюдение осуществляется в радиодиапазоне электромагнитных волн с помощью способов и средств радиолокации и радиотеплолокации.

Для получения радиолокационного изображения в радиолокаторе формируется зондирующий узкий, сканирующий по горизонтали и вертикали луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта

радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикатора, который перемещаясь синхронно с зондирующим лучом «рисует» на экране изображение объекта.



Отраженная энергия в радиодиапазоне пропорциональна площади поверхности и конфигурации объекта, электрической проводимости поверхности. Отражательная способность объекта или его элементов характеризуется эффективной площадью рассеяния.

Основными показателями радиолокационных средств наблюдения являются:

- дальность наблюдения; Дальность радиолокационного наблюдения зависит от излучаемой радиолокатором энергии (мощности передатчика локатора) и характеристик среды распространения электромагнитной волны. Ослабление электромагнитной волны при ее распространении определяется длиной волны и степенью ослабления ее в атмосфере. Чем короче длина волны, тем прямолинейнее ее путь распространения и тем больше она затухает в атмосфере. Но одновременно тем выше может быть обеспечена разрешающая способность радиолокатора на местности.

- разрешающая способность на местности. Разрешение радиолокатора на местности определяется величиной пятна, которое создает луч радиолокационной станции при облучении поверхности объекта или местности. Пятно тем меньше, чем уже диаграмма направленности антенны радиолокатора. Последняя, в свою очередь, определяется соотношением геометрических размеров конструкции антенны и длины волны.

По дальности действия наземные радиолокаторы различаются на малой, средней, большой дальности и сверхдальнего действия. РЛС ***малой дальности*** применяют для обнаружения людей и транспортных средств на расстоянии в сотни метров, ***средней*** - единицы км, ***большой*** - десятки км. Точность определения координат наземных РЛС составляет по дальности 10-20% и около градуса по азимуту.

Сверхдальные РЛС используют эффект распространения на большие расстояния не только в прямом, но и обратном направлениях. Отражаясь от объектов на земной поверхности на удалении 800-4000 и более км от РЛС, электромагнитные волны, несущие информацию об их демаскирующих признаках, принимаются и регистрируются приемником радиолокатора.

В РЛС БО применяются два вида антенн: **вдольфюзеляжные** и с **синтезированной** (искусственной) апертурой антенны (РСА).

Принцип работы радиолокатора бокового обзора иллюстрируется на рис.

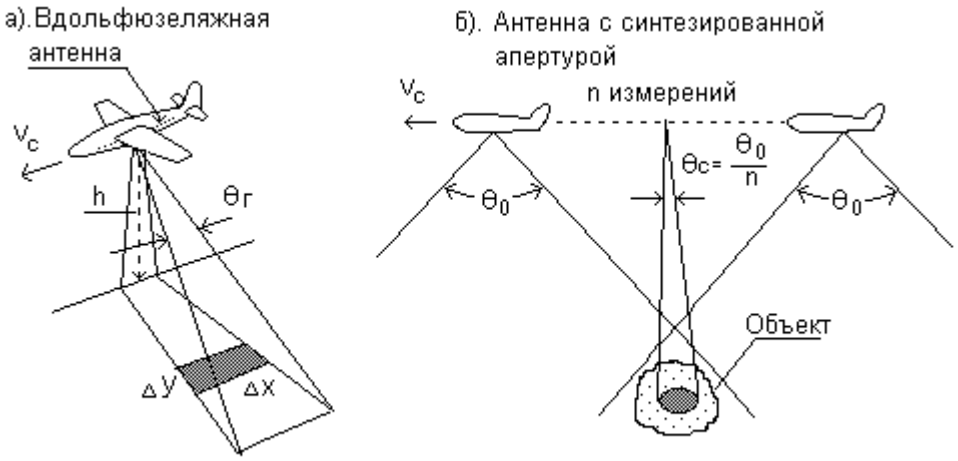


Рис. Принцип работы радиолокатора бокового обзора

Элементы антенны первого вида размещают вдоль фюзеляжа самолета с обеих его сторон или в подвесном контейнере-обтекателе. Благодаря этому размер антенны можно увеличить до 15 м. Такая антенна создает в боковом направлении узкую (доли градусов) диаграмму направленности в горизонтальной плоскости и широкую - в вертикальной.

В текущий момент времени она облучает на земной поверхности площадку шириной Dx и длиной Dy (см. рис.). Так как зондирующий сигнал проходит до элементов этой площадки и после отражения к антенне разные пути, то лучи в точке приема имеют разные фазы. На приемной стороне сигналы, отраженные от разных участков площадки, упорядочиваются по фазе, в результате чего обеспечивается возможность увеличить разрешение в вертикальной плоскости до значения, соответствующего шагу дискретизации фазы. Величина же шага ограничивается точностью определения точности фазы и возможностями бортового компьютера.

Просмотр земной поверхности по направлению полета самолета или космического аппарата производится за счет движения носителей РЛС БО с разрешением на местности, соответствующему ширине диаграммы направленности антенны в горизонтальной плоскости - по азимуту.

В РЛС применяется небольшая антенна, широкая диаграмма направленности которой неподвижна относительно самолета и направлена перпендикулярно линии полета. При полете самолета антенна РЛС последовательно занимает в пространстве положения на прямой траектории полета самолета, эквивалентные положениям элементам гипотетической антенной решетки. В результате запоминания сигналов, последовательно принимаемых антенной в каждой точке траектории полета самолета, и их когерентного суммирования достигается существенное повышение разрешающей способности на местности.

Радиотеплолокационное наблюдение объектов осуществляется с помощью специальных радиоприемных устройств, называемых радиометрами. В радиометре производится суммирование по мощности тепловых радиоизлучений поверхности объекта наблюдения, детектирование сигнала, усиление видеосигнала и формирование радиотеплолокационного изображения на индикаторе (экране) аналогично формированию изображения на индикаторе радиолокационной станции. В связи с тем, что параметры антенны радиометра оказывают более существенное влияние на его дальность и разрешение, к антенне радиометра предъявляются более жесткие требования к максимуму коэффициента усиления и минимуму уровня боковых лепестков. Применяются зеркальные параболические, линзовые и многоэлементные антенны.

Для снижения собственных тепловых шумов во входных каскадах радиометра используются слабошумящне квантомеханические и параметрические усилители, различные способы компенсации помех в цепях радиометра и др.
Учитывая невысокие по сравнению с активной радиолокацией дальность и разрешение радиометров, возможности радиотеплолокации по добыванию видовых демаскирующих признаков весьма ограничены.

Радиолокационное и радиотепловое наблюдение осуществляется в радиодиапазоне электромагнитных волн с помощью способов и средств радиолокации и радиотепловидения.

Для получения радиолокационного изображения в радиолокаторе формируется зондирующий узкий сканирующий (перемещающейся по определенному закону по горизонтали и вертикали) луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикатора, который перемещаясь синхронно с зондирующим лучем «рисует» на экране изображение объекта. Принципы радиолокационного наблюдения показаны на рис.

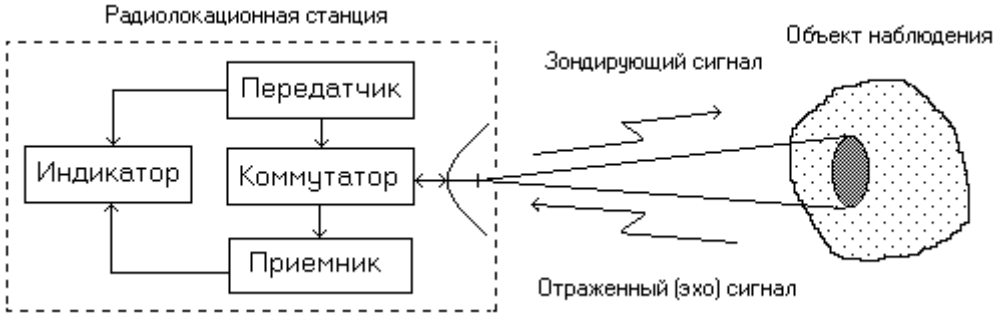


Рис. Принципы радиолокационного наблюдения.

Радиолокационное изображение существенно отличается от изображения в оптическом диапазоне. Различие обусловлено разными свойствами отражающей поверхности объектов в оптическом и радиодиапазонах.

Отраженная энергия в радиодиапазоне пропорциональна площади поверхности и конфигурации объекта, электрической проводимости поверхности. Отражательная способность объекта или его элементов характеризуется эффективной площадью рассеяния.

Эффективная площадь рассеяния равна площади идеальной плоской поверхности, перпендикулярной к направлению облучения и помещенной в точке нахождения объекта, которая создает у приемной антенны радиолокатора такую же плотность потока мощности, как реальный объект.

Основными показателями радиолокационных средств наблюдения являются следующие:
- дальность наблюдения;
- разрешающая способность на местности.

Дальность радиолокационного наблюдения зависит от излучаемой радиолокатором энергии (мощности передатчика локатора) и характеристик среды распространения электромагнитной

волны. Ослабление электромагнитной волны при ее распространении определяется длиной волны и степенью ослабления ее в атмосфере. Чем короче длина волны, тем прямолинейнее ее путь распространения и тем больше она затухает в атмосфере. Но одновременно тем выше может быть обеспечена разрешающая способность радиолокатора на местности.

Разрешение радиолокатора на местности определяется величиной пятна, которое создает луч радиолокационной станции при облучении поверхности объекта или местности. Пятно тем меньше, чем уже диаграмма направленности антенны радиолокатора. Последняя, в свою очередь, определяется соотношением геометрических размеров конструкции антенны и длины волны. Кроме того, следует иметь ввиду, что электромагнитная волна отражается от объекта или его деталей, если их размеры, по крайней мере, соизмеримы с длиной волны. Если размеры их значительно меньше, то волна эти объекты огибает. В связи с этими с этими соображениями наиболее широко в радиолокации применяется сантиметровый диапазон с тенденцией перехода в мм-диапазон.

По дальности действия наземные радиолокаторы различаются на малой, средней, большой дальности и сверхдальнего действия. РЛС малой дальности применяют для обнаружения людей и транспортных средств на расстоянии в сотни метров, средней - единицы км, большой - десятки км. Точность определения координат наземных РЛС составляет по дальности 10-20% и около градуса по азимуту.

Сверхдальные РЛС используют эффект, открытый в 60 е годы Н. И. Кабановым. Этот эффект состоит в способности радиоволн в декаметровом диапазоне распространяться на большие расстояния не только в прямом, но и обратном направлениях. Отражаясь от объектов на земной поверхности на удалении 800-4000 и более км от РЛС, электромагнитные волны, несущие информацию об их демаскирующих признаках, принимаются и регистрируются приемником радиолокатора. Однако из-за нестабильности ионосферы разрешение таких РЛС значительно хуже, чем у надгоризонтных радиолокаторов.

Повышение разрешающей способности радиолокаторов без значительного увеличения размеров антенны, что особенно важно для воздушного и космического радиолокационного наблюдения, обеспечивается в радиолокационных станциях бокового обзора (РЛС БО). Они размещаются на самолетах и разведывательных КА.

В РЛС БО применяются два вида антенн: вдольфюзеляжные и с синтезированной (искусственной) апертурой антенны (РСА).

Принцип работы радиолокатора бокового обзора иллюстрируется на рис.

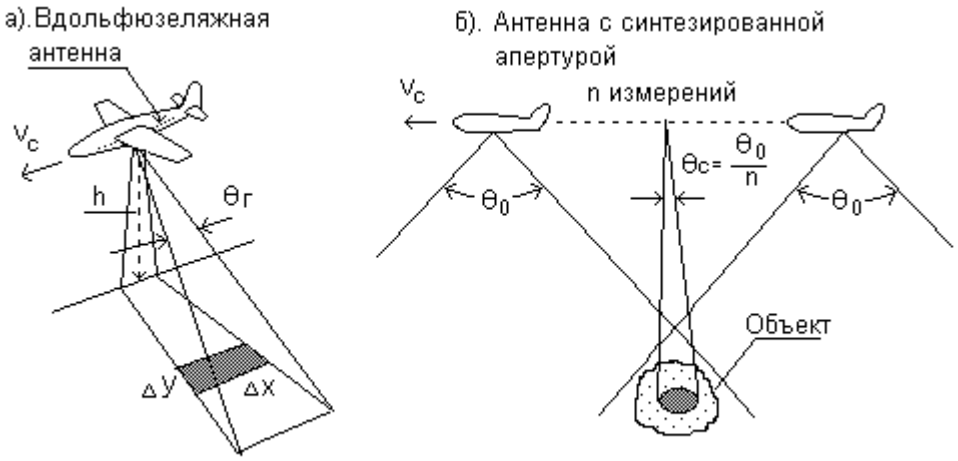


Рис. Принцип работы радиолокатора бокового обзора

Элементы антенны первого вида размещают вдоль фюзеляжа самолета с обеих его сторон или в подвесном контейнере-обтекателе. Благодаря этому размер антенны можно увеличить до 15 м. Такая антенна создает в боковом направлении узкую (доли градусов) диаграмму направленности в горизонтальной плоскости и широкую - в вертикальной. В текущий момент времени она облучает на земной поверхности площадку шириной Δx и длиной Δy (см. рис.3.7). Так как зондирующий сигнал проходит до элементов этой площадки и после отражения к антенне разные пути, то лучи в точке приема имеют разные фазы. На приемной стороне сигналы, отраженные от разных участков площадки, упорядочиваются по фазе, в результате чего обеспечивается возможность увеличить разрешение в вертикальной плоскости до значения, соответствующего шагу дискретизации фазы. Величина же шага ограничивается точностью определения точности фазы и возможностями бортового компьютера.

Просмотр земной поверхности по направлению полета самолета или космического аппарата производится за счет движения носителей РЛС

БО с разрешением на местности, соответствующему ширине диаграммы направленности антенны в горизонтальной плоскости - по азимуту.

Повышение угловой разрешающей способности РЛС с синтезированной апертурой антенны основано на формировании узкой диаграммы направленности по азимуту с помощью искусственно создаваемой антенной решетки. Диаграмма направленности антенной решетки, формируемой в результате когерентного (с учетом фазы) сложения радиоволн от n одинаковых ее элементов размером d, что и антенна размером nd.

В РЛС применяется небольшая антенна, широкая диаграмма направленности которой неподвижна относительно самолета и направлена перпендикулярно линии полета. При полете самолета антенна РЛС последовательно занимает в пространстве положения на прямой траектории полета самолета, эквивалентные положениям элементам гипотетической антенной решетки. В результате запоминания сигналов, последовательно принимаемых антенной в каждой точке траектории полета самолета, и их когерентного суммирования достигается существенное повышение разрешающей способности на местности. Размер решетки (синтезированной апертуры) соответствует длине участка траектории, на котором производится запоминание и

когерентное суммирование сигналов. Используя этот метод, можно увеличить разрешающую способность РЛС по азимуту в 100 и более раз.

3.2. Способы и средства перехвата сигналов.

Перехват носителей в виде электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией осуществляют органы добывания радио и радиотехнической разведки. При перехвате решаются следующие основные задачи:
- поиск по демаскирующим признакам сигналов с информацией в диапазоне частот, в которых они могут;
- обнаружение и выделение сигналов, интересующих органы добывания;
- прием (селекция, усиление) сигналов и съем с них информации;
- анализ технических характеристик принимаемых сигналов;
- определение местонахождения (координат) источников представляющих интерес сигналов;
- обработка полученных данных с целью формирования первичных признаков источников излучения или текста перехваченного сообщения.

Упрощенная структура типового комплекса средств приведена на рис.



Рис. Структура комплекса средств перехвата

Типовой комплекс включает:
- приемные антенны;
- радиоприемник;
- анализатор технических характеристик сигналов;
- радиопеленгатор;
- устройство обработки сигналов;
- устройство индикации и регистрации.

Антенна предназначена для преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствует аналогичным характеристикам электромагнитной волны.

В радиоприемнике производится селекция сигналов по частоте, усиление и детектирование (демодуляция) выделенных радиосигналов с целью получения сигнала на носителе в виде электрических первичных сигналов: речевых, цифровых данных, видеосигналов.

Для анализа радиосигналов после селекции и усиления они подаются на входы комплекса измерительной аппаратуры, осуществляющей автоматическое или автоматизированное

измерение их параметров: частотных, временных, энергетических, вида модуляции, видов и структуры кодов и др. Эти комплексы различаются по диапазонам частот, функциям, принципам построения (аналоговые, цифровые).

Радиопеленгатор определяет направление на источник излучения (пеленг) или его координаты.

Устройство обработки и регистрации производит первичную обработку информацию (сведений и данных) и регистрирует ее для последующей обработки.

Каждое из этих средств характеризуется набором определенных функций и параметров.

а) Антенны

Антенны преобразуют энергию электромагнитной волны в электрические сигналы и представляют конструкцию из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования. Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн, классификация основных из которых представлена на рис.

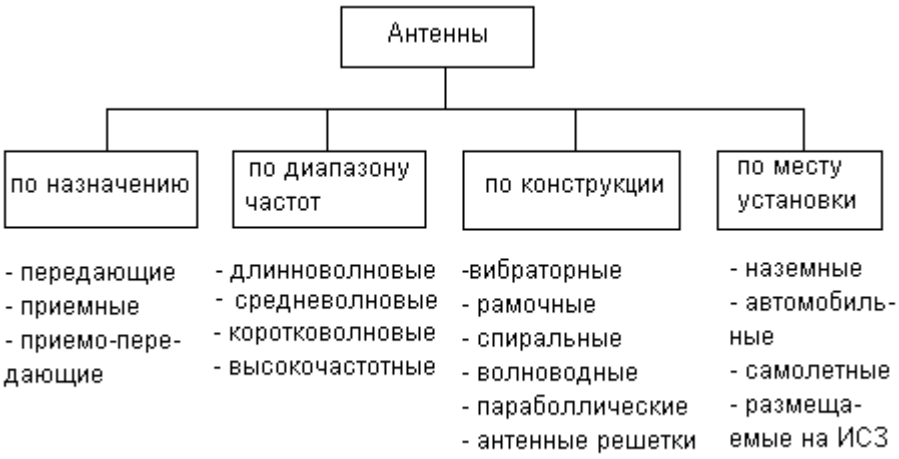


Рис. Классификация антенн

Назначение передающих и приемных антенны ясно из их наименований. По своим основным электрическим параметрам они не отличаются. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находящиеся под высоким напряжением.

Эффективность антенн зависит от согласования размеров элементов антенны с длинами излучаемых или принимаемых волн. Длина согласованной с длиной волны электромагнитного колебания штыревой антенны близка к $\lambda/4$, где λ - длина рабочей волны. Поэтому размеры и конструкция антенн отличаются как для различных диапазонов частот, так и внутри диапазонов.

Если для стационарных антенн требование к геометрическим размерам антенны может быть достаточно просто выполнено для коротких и ультракоротких волн, то для антенн, устанавливаемых на мобильных средствах, оно неприемлемо. Например, рациональная длина антенны для обеспечения связи на частоте 30 МГц составляет 2.5 м, что неудобно для пользователя. Поэтому применяют укороченные антенны, но при этом уменьшается их КПД. По данным [16] укорочение антенны в 2 раза уменьшает КПД до 60%, в 5 раз (до 50 см) - до 10%, а КПД антенны, укороченной в 10 раз, составляет всего около 3% от рационального варианта.

По конструкции антенны разделяются на проволочные (вибраторные), рупорные, параболические, рамочные, спиральные, антенные решетки и различные их комбинации.

Возможности антенн как приемных, так и передающих определяются следующими характеристиками:
- диаграммой направленности;
- коэффициентом полезного действия;
- коэффициентом направленного действия;
- коэффициентом усиления;
- полосой частот.

Диаграмма направленности представляет графическое изображение уровня принимаемого сигнала от угла поворота антенны в горизонтальной и вертикальной плоскостях. Диаграммы изображаются в прямоугольных и полярных координатах (см. рис.).

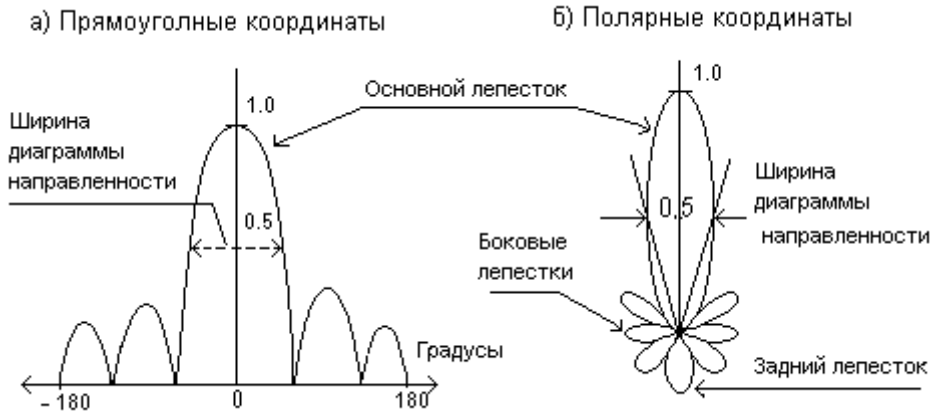


Рис. Диаграмма направленности антенн.

Они могут иметь разнообразный и изрезанный характер, определяемый механической конструкцией и электрическими параметрами. Лепесток диаграммы направленности с максимумом мощности излучаемого или принимаемого электромагнитного поля называется главным или основным лепестком, остальные боковыми и задними. Соотношение между величинами мощности основного лепестка по сравнению с остальными характеризует направленные свойства антенны. Ширина главного лепестка диаграммы измеряется углом между прямыми, проложенными из начала полярных координат до значений диаграммы, соответствующих половине максимальной мощности излучения или 0.7 напряжения электрического сигналов приемной антенны. Чем уже ширина диаграммы направленности антенны, тем выше ее коэффициент направленного действия.

Коэффициент направленного действия (КНД) определяет величину энергетического выигрыша, который обеспечивает направленная антенна по сравнению с ненаправленной.

Потери электрической энергии в антенне оцениваются коэффициентом полезного действия (КПД), равного отношению мощности сигнала на выходе реальной антенны к мощности сигнала идеальной антенны без потерь.

Произведение этих двух коэффициентов определяет коэффициент усиления антенны (КУ). Так как КНД >1, а КПД <1, то коэффициент усиления в зависимости от значений сомножителей может теоретически принимать значения как меньше, так и больше 1. Чем выше КУ, тем больший энергетический эффект обеспечивает антенна, но тем точнее необходимо ориентировать направление основного лепестка на источник излучения. Для параболической антенны коэффициент усиления антенны рассчитывается по формуле

$$КУ=4\pi S_{эф}/\lambda^2,$$

где $S_{эф}$ - эффективная площадь зеркала антенны;
λ - длина электромагнитной волны.
Для линейных антенн (например, вибраторов) КУ характеризуется действующей высотой или длиной $h_a=E_a/E$, где E_a - максимальное значение наводимой в антенне электродвижущей силы, E - напряженность электромагнитного поля в точке приема. Полоса частот, в пределах которых сохраняются заданные технические характеристики антенны, называется полосой ее пропускания.

Создание антенн с высоким коэффициентом усиления и широкой полосой пропускания представляет основную проблему в области конструирования антенн. Чем выше КУ, тем труднее обеспечить широкополосность антенны. В зависимости от полосы пропускания антенны разделяются на узкополосные, широкополосные, диапазонные и широкодиапазонные.

Узкополосные антенны обеспечивают прием сигналов в диапазоне 10% от основной частоты. У широкополосных антенн эта величина увеличивается до (10-50)%, диапазонные антенны имеют коэффициент перекрытия (отношение верхней частоты полосы пропускания антенны к нижней) составляет 1.5-4, а у широкополосных антенн это отношение достигает значений в интервале 4-20.

Совокупность однотипных антенн, расположенных определенным образом в пространстве, образуют антенную решетку. Сигнал антенной решетки соответствует сумме сигналов от отдельных антенн. Различают линейные (одномерные) и плоские (двухмерные) антенные решетки. Антенные решетки, у которых можно регулировать фазы сигналов отдельных антенн, называют фазированными антенными решетками. Путем изменения фаз суммируемых сигналов можно менять диаграмму направленности в горизонтальной и вертикальной плоскостях и производить быстрый поиск сигнала по пространству и ориентацию антенны на источник излучения.

б) Радиоприемник

Радиоприемник - основное техническое средство перехвата, осуществляющего поиск, селекцию, прием и обработку радиосигналов. В состав его входят устройства, выполняющие:
- перестройку частоты настройки приемника и селекцию (выделение) нужных радиосигналов;

- усиление выделенных сигналов;
- детектирование (съем информации);
- усиление видео или низкочастотного первичного сигнала.

Различают два вида радиоприемников: прямого усиления и супергетеродинные. Появившиеся первыми приемники прямого усиления уступили супергетеродинным почти во всех радиодиапазонах, за исключением сверхвысоких частот. Такая тенденция объясняется более высокой селективностью и чувствительностью супергетеродинного радиоприемника по сравнению с приемником прямого усиления.

В приемниках прямого усиления, как следует из названия, сигнал на входе приемника (выходе антенны) селектируется и усиливается без изменения его частот. Качество информации, снимаемой с этого сигнала, тем выше, чем меньше уровень помех (сигналов различной природы с частотами, близкими частоте настройки приемника). В идеале цепи селекции должны обеспечивать П - образную форму с полосой пропускания, равной ширине спектра селектируемого сигнала.

Такие фильтры имеют многозвенную, достаточно сложную конструкцию из тщательно настраиваемых LC - элементов или реализуются с использованием поверхностных акустических волн.

Сложность проблемы обеспечения избирательности в радиоприемниках прямого усиления обусловлена техническими трудностями создания одновременно перестраиваемых по частоте узкополосных фильтров с высокими показателями по селективности, в особенности при их промышленном производстве. Только на сверхвысоких частотах удалось достигнуть высоких показателей по чувствительности и избирательности благодаря применению в широкополосных цепях высокой частоты специальных материалов и устройств: фильтров из железоиттриевого граната и малощумящих ламп бегущей волны.

В супергетеродинном приемнике проблема одновременного обеспечения высоких значений чувствительности и селективности решена путем преобразования принимаемого высокочастотного сигнала после его предварительной селекции и усиления в усилителе высокой частоты в сигнал постоянной частоты, называемой промежуточной частотой (см. рис.).

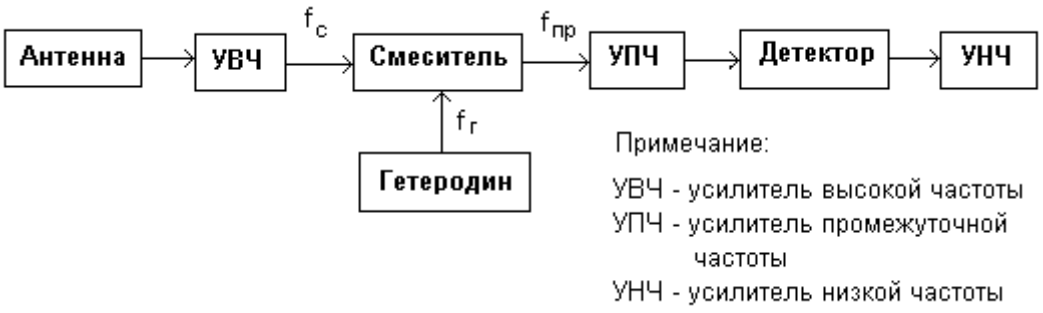


Рис. Структура супергетеродинного приемника.

После преобразования усиление и селекция выполняются применительно к сигналам промежуточной частоты. Для постоянной промежуточной частоты задачи по обеспечению высокой избирательности и чувствительности решаются проще и лучше. Преобразователь

частоты состоит их гетеродина и смесителя. Гетеродин представляет собой перестраиваемый вручную или автоматически высокочастотный генератор гармонического колебания с частотой, отличающейся от частоты принимаемого сигнала на величину промежуточной частоты. Процесс преобразования частоты происходит в смесителе, основу которого составляет нелинейный элемент (полупроводниковый диод, транзистор, радиолампа). На него поступают принимаемый сигнал с частотой fc и гармонический сигнал гетеродина с частотой $f_г$. На выходе смесителя создается множество комбинаций гармоник принимаемого сигнала и колебаний гетеродина, в том числе на промежуточной частоте $f_п=f_c- f_г$. Селективные фильтры усилителя промежуточной частоты пропускают только сигналы промежуточной частоты, которые усиливаются до величины, необходимой для нормальной работы детектора. Однако супергетеродинному приемнику присущ ряд недостатков, вызванных процессом преобразования частоты. Они состоят в том, что фильтры усилителя промежуточной частоты пропускают не только полезные сигналы, частота которых равна $f_c=f_г+f_п$,, но и ложные с частотой $f_л= f_г - f_п$, симметричной (“зеркальной”) по отношению к частоте гетеродина $f_г$. Помехи на “зеркальной” частоте ослабляются путем двойного или даже тройного преобразования частот в супергетеродинном приемнике. Промежуточная частота каждого последующего преобразования понижается. В результате этого первую промежуточную частоту можно без ущерба для избирательности приемника выбрать достаточно высокой. При больших значениях промежуточной частоты “зеркальная” частота существенно отличается (на удвоенную промежуточную частоту) от сигнала и подавляется входными фильтрами радиоприемника.

Возможности радиоприемника определяются следующими техническими характеристиками:
- диапазоном принимаемых частот;
- чувствительностью;
- избирательностью;
- динамическим диапазоном;
- показателями качества принимаемой информации;
- эксплуатационными параметрами.

Диапазон принимаемых частот обеспечивается шириной полосы пропускания селективных элементов входных фильтров и фильтров усилителя высокой частоты. Настройка же приемника на нужную частоту производится путем механической или электронной перестройкой частоты гетеродина. При поиске сигналов важной характеристикой является скорость перестройки, которая в панорамных приемниках (приемниках для быстрого обзора радиодиапазонов) достигает сотни МГц за 1 мксек.

Чувствительность радиоприемника оценивается минимальной мощностью или напряжением сигнала на его входе, при которой на выходе приемника достигается отношение сигнал/помеха и мощность (напряжение), необходимые для нормальной работы оконечной аппаратуры или восприятия информации человеком. Такая чувствительность называется реальной. Предельная чувствительность соответствует мощности (напряжения) входного сигнала, равного мощности шумов входных цепей радиоприемника. Информация полезного сигнала мощностью менее мощности шумов радиоприемника настолько сильно ими искажается, что передача информации возможна только при кодировании ее специальными помехоустойчивыми кодами.

В диапазонах дециметровых и более коротких волн чувствительность измеряют в ваттах или децибелах по отношению к уровню в 1 мВт (дБм), на метровых и более длинных - в микровольтах (мкВ). Реальная чувствительность современных профессиональных

супергетеродинных приемников дециметровых и сантиметровых волн находится в пределах 10^{-12}-10^{-14} Вт, приемников метровых и более длинных волн составляет 0.1-10 мкВ.

Избирательность приемника оценивается параметрами амплитудно-частотной характеристики (АЧХ) его селективных цепей, определяющей зависимость коэффициента усиления приемного тракта от частоты. Избирательность приемника максимальная, когда его амплитудно-частотная характеристика повторяет форму спектра принимаемого сигнала. В этом случае будут приняты все его спектральные составляющие, но не пропущены спектральные составляющие других сигналов (помех). Практически реализовать это требование чрезвычайно трудно, так как спектр сигналов с различной информацией имеет изрезанную постоянно меняющуюся форму и существуют большие технически проблемы при формировании амплитудно-частотной характеристики сложной заданной формы.

Амплитудно-частотная характеристика (АЧХ) радиоприемника характеризует величину пропускания его селективных цепей в зависимости от частоты колебания сигнала. В качестве идеальной АЧХ рассматривается П образная форма с шириной, равной средней ширине спектра сигнала.

Избирательность реального приемника оценивается двумя основными показателями: шириной полосы пропускания и коэффициентом прямоугольности АЧХ радиоприемника, реальная форма которой имеет колоколообразный вид.

Ширина полосы пропускания определяется на уровне 0.7 по напряжению, а коэффициент прямоугольности - отношением полосы пропускания на уровне 0.1 к полосе пропускания на уровне 0.7. Чем более пологой является АЧХ радиоприемника, тем шире полоса пропускания на уровне 0.1 по отношению к уровню 0.7 и тем больше величина коэффициента прямоугольности. Коэффициент пропускания позволяет количественно оценить пологий характер амплитудно-частотной характеристики радиоприемника. Чем ближе коэффициент прямоугольности АЧХ к 1, тем круче ее скаты и тем меньше помех «пролезет» по краям полосы пропускания. С целью уменьшения мощности помех, прошедших в тракт приемника, ширину его полосы пропускания устанавливают соответствующей ширине спектра сигнала. В приемниках для приема сигналов, существенно отличающихся по ширине, например, речи и телеграфа, ширину полос пропускания различных селективных цепей изменяют путем коммутации селективных элементов (катушек индуктивности, конденсаторов).

Так как активные элементы усилительных каскадов радиоприемника (транзисторы, диоды и др.) имеют достаточно узкий интервал значений входных сигналов, при которых обеспечивается линейное усиление сигналов, то при обработке сигналов с амплитудой вне этих интервалов возникают их нелинейные искажения и, следовательно, искажение информации. В реальных условиях уровни сигналов на входе приемников, используемых для добывания информации, существенно отличаются. Например, громкость речи при приеме сигналов закладных устройств меняется в широких пределах при перемещении говорящего человека в помещении. Динамический диапазон характеризует возможности приемника по безискаженному приему сигналов различной мощности. Величина динамического диапазона оценивается отношением максимального уровня к минимальному уровню принимаемого сигнала и измеряется в децибелах. При недостаточном динамическом диапазоне возникают искажения электрических сигналов, соответствующих громким звукам.

Для повышения динамического диапазона современные радиоприемники содержат устройство

автоматической регулировки усиления (АРУ) приемного тракта в соответствии с уровнем принимаемого сигнала.

Несоответствие амплитудно-частотной и фазовой характеристик, динамического диапазона радиоприемника текущим характеристикам сигнала приводят к частотным, фазовых и нелинейным искажениям сигнала и потере информации.

Частотные искажения вызываются подавлением или изменениями составляющих спектра входного сигнала. Из-за частотных искажений сигнал на входе демодулятора приобретает форму, отличающуюся от входной.

Фазовые искажения сигнала возникают из-за нарушений фазовых соотношений между отдельными спектральными составляющими сигнала при прохождении его цепям тракта приемника.

Искажения, проявляющиеся в появлении в частотном спектре выходного сигнала дополнительных составляющих, отсутствующих во входном сигнале, называются нелинейные. Нелинейные искажения вызывают элементы радиоприемника, имеющие нелинейную зависимость между выходом и входом. Они возникают при превышении отношения значений максимальной и минимальной напряженности электромагнитной волны в месте приема динамического диапазона радиоприемника.

Эти виды искажений приводят к изменению информационных параметров сигнала на входе демодулятора и, как следствие, к искажению информации после демодуляции. Кроме указанных электрических характеристик возможности радиоприемников оцениваются также по их надежности, оперативности управления, видам электропитания и потребляемой мощности, массо-габаритным показателям.

Особенностью этих радиоприемников является возможность очень быстрой (электронной) перестройки в широком диапазоне частот. Кроме того, наиболее совершенные из сканеров содержат устройство «памяти», которое запоминает вводимые априори, а также в процессе поиска, частоты радиосигналов, не представляющие интерес для оператора. В результате такого запоминания резко сокращается время просмотра широкого диапазона частот.

Средства измерения признаков сигнала включают большой набор различных программно-аппаратных устройств и приборов, в том числе устройства панорамного обзора и анализа спектра, измерители временных параметров дискретных сигналов, определители видов модуляции и кода.

Разрешение по наклонной дальности в РСА обеспечивается, как и в других РЛС БО, за счет импульсного режима их работы.

При наблюдении земной поверхности с помощью РСА предъявляются жесткие требования к прямолинейности траектории полета самолета, к стабильности амплитудно-фазовых характеристик приемопередающего тракта РЛС и устройств обработки сигналов, параметров среды распространения и характеристик отражения радиоволн наблюдаемых объектов. Для цифровой обработки сигналов требуется так же большая память бортового компьютера.

Специфика защиты от радиолокационного наблюдения вызвана особенностями получения радиолокационного изображения. Структура радиолокационного изображения зависит от разрешающей способности радиолокатора, электрических свойств отражающей поверхности объектов и фона, от степе-ни ее неровностей (шероховатости), от длины и поляризации волны, облучающей объект, угла падения электромагнитных волн на поверхность объекта. Разрешающая способность локатора определяется в основном шириной диаграммы направленности его антенны, как известно, совмещающей в од-ной конструкции функции передающей и приемной.

В настоящее время наиболее широко используется для радиолокации см-диапазон. Разрешение на местности в этом диапазоне самолетных (бортовых) радиолокаторов составляет единицы метров. С целью повышения разрешающей способности радиолокаторов применяется мм-диапазон, в котором проще создать антенны приемлемых размеров с более узкой диаграммой направленности. Но мм-волны сильнее затухают в атмосфере, что приводит к снижению дальности наблюдения. Кроме того, более длинные волны имеют лучшую проникающую способность в поверхность объекта, что затрудняет его маскировку.

Таким образом, радиолокационное изображение существенно отличается от изображения в оптическом диапазоне и используется разведкой для получения дополнительных демаскирующих признаков на существенно большем удалении от объекта и в неблагоприятных климатических условиях.

Указанные особенности учитываются при организации защиты информации. Меры по защите направлены на снижение эффективной поверхности рассеяния(ЭПР) объекта в целом и его характерных участков, содержащих информативные демаскирующие признаки. Структурное скрытие обеспечивается в результате изменения структуры изображения защищаемого объекта на экране локатора путем:

- покрытия объекта экранами, изменяющими направления распространения отраженного электромагнитного поля;
- размещения в местах расположения объекта дополнительных отражателей;
- генерирования радиопомех.

В качестве дополнительных радиоотражателей применяются уголковые, линзовые, дипольные отражатели и переизлучающие антенные решетки (ПАР).

Для энергетического скрытия объектов от радиолокационного наблюдения его поверхность покрывают материалами, обеспечивающими градиентное и интерференционное поглощение облучающей электромагнитной энергии.

Другой способ энергетического скрытия, который широко применяется для защиты объектов от радиолокационного наблюдения, — генерация помех. Простейшей помехой является гармоническое колебание на частоте РЛС, создаваемое генератором помех в месте нахождения защищаемого объекта. Так как диаграмма направленности антенны РЛС имеет, как правило, боковые лепестки, то такая помеха создает шумовую засветку экрана локатора.

Более сложной по структуре является модулированная помеха с одним или несколькими изменяющимися параметрами. Модулированная помеха бывает непрерывной и импульсной и обладает спектром, близким к спектру излучения РЛС. По эффекту воздействия помехи разделяются на маскирующие изображение объекта путем зашумления экрана РЛС и имитирующие на нем ложные световые пятна. изменяя структуру и время задержки имитационной помехи, можно менять форму, место и характер движения ложной засветки на экране локатора.

Средства противодействия перехвату радиосигналов. При перехвате сигналов функциональных каналов связи передатчики этих каналов являются одновременно источниками радиоэлектронных каналов утечки информации. В соответствии с общими принципами защиты информации защита передаваемой информации в этом случае заключается в е, криптографическом либо техническом закрытии (скремблировании), поскольку противодействовать перехвату радиосигналов крайне

затруднительно. Наиболее простым способом скремблирования является частотная и временная инверсии речевого сигнала. Частотная инверсия заключается в повороте спектра речевого сигнала вокруг некоторой центральной частоты. Временная инверсия заключается в запоминании в памяти передающего скремблера отрезка речевого со-общения и считывание его с конца кадра. Для достижения неразборчивости речи продолжительность кадра должна быть не менее 250 мс.

Акустические каналы. В акустических каналах утечки информации средой распространения речевых сигналов является воздух и для их перехвата используются высокочувствительные микрофоны и специальные направленные микрофоны, которые соединяются со специальными миниатюрными передатчиками. Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами (ЗУ) перехвата речевой информации. Перехваченная ЗУ речевая информация может передаваться по радиоканалу, сети электропитания, оптическому (ИК) каналу, соединительным линиям вспомогательных технических средств (ВТСС), посторонним проводникам, инженерным коммуникациям в ультразвуковом (УЗ) диапазоне частот, телефонной линии с вызовом от внешнего телефонного абонента. Прием информации, передаваемой закладными устройствами, осуществляется, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн. Использование портативных диктофонов и закладных устройств требует проникновения в контролируемое помещение. В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

Виброакустические каналы. В виброакустических каналах утечки информации средой распространения речевых сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.). Для перехвата речевых сигналов используются вибродатчики (акселерометры). Вибродатчик, соединенный с электронным усилителем, называют электронным стетоскопом. Электронный стетоскоп позволяет осуществлять прослушивание речи с помощью головных телефонов и ее запись на диктофон. По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. Для передачи информации используется радиоканал, а устройства называются радиостетоскопами. Еще используются закладные устройства с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн и по ультразвуковому каналу (по инженерным коммуникациям).

Акустоэлектрические каналы. Акустоэлектрические каналы утечки информации возникают за счет преобразований акустических сигналов в электрические. Некоторые элементы ВТСС, трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов и т.п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. ВТСС могут содержать акустоэлектрические преобразователи. К ним относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Перехват акустоэлектрических колебаний осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей.

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

выделяется речевая информация. Для перехвата используются сложные лазерные системы.

Акустоэлектромагнитный канал (параметрический канал).Акустоэлектромагнитный, или как его еще называют параметрический канал утечки информации, образуется в результате воздействия акустического поля на элементы высокочастотных генераторов. В результате такого воздействия происходят незначительные изменения взаимного расположения элементов схем, проводов в катушках индуктивности (межвиткового расстояния), дросселей, расстояний между пластинами воздушных конденсаторов и т. п., что может привести к изменениям параметров высокочастотного сигнала, например к модуляции его информационным сигналом. Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки.

Параметрический канал утечки информации может быть реализован и путем “высокочастотного облучения” помещения, где установлены полуактивные закладные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического (речевого) сигнала.

Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленной антенной и приемник.

Для подслушивания применяют следующие технические средства:

- − акустические приемники, в том числе с направленными микрофонами;
- − приемники опасных сигналов (радио и электросигналов каналов связи и побочных излучений и наводок);
- − акустические закладные устройства;
- − лазерные системы подслушивания;
- − устройства подслушивания путем высокочастотного навязывания.

Акустические приемники обеспечивают селекцию акустических сигналов, распространяющихся в атмосфере, воде, твердых телах, преобразуют их в электрические сигналы, усиливают иобрабатывают электрические сигналы и преобразуют их в акусти- ческую волну для восприятия информации слуховой системой человека. Сигналы на выходе приемника могут записываться на носитель.
Типовая структура акустического приемника приведена на рис.

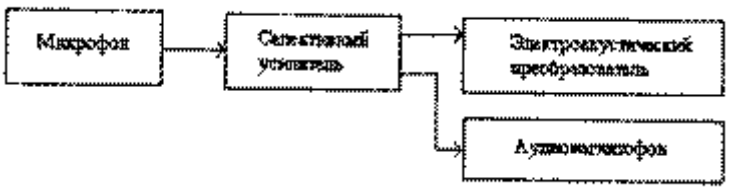
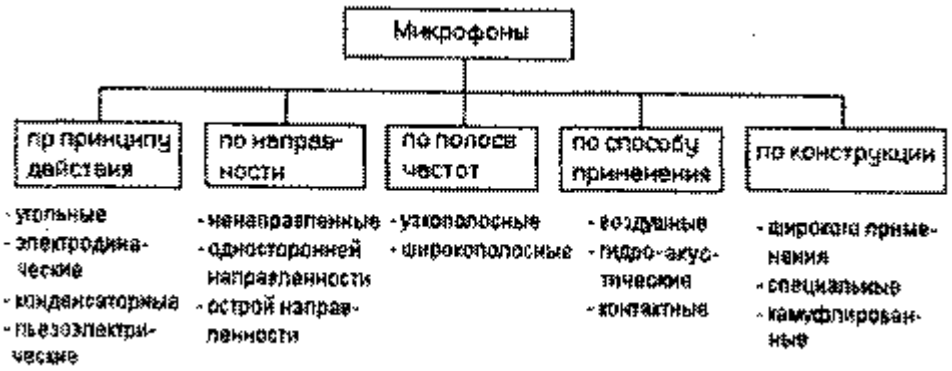


Рис. Структурная схема акустического приемника

Классификация микрофонов



Действие угольного микрофона: при воздействии звукового давления на диафрагму угольного микрофона она совершает колебания. В такт с этими колеба- ниями изменяется силасжатия зерен угольного порошка (засыпки). Вследствие этого изменяется сопротивление засыпки между электродами. При постоянном напряжении, приложенном к этим электродам,изменяется и величина тока, протекающего через микрофон. Если включить микрофон в первичную обмотку трансформатора, то на зажимах его вторичной обмотки будет возникатьпеременное напряжение, соответствующее воздействующему на микрофон акустическому сигналу.

Действие **электродинамического преобразователя** основано на использовании явления электромагнитной индукции. При воздействии на диафрагму звукового давления, она вместе сподвижной катушкой совершает колебания в магнитном поле, создаваемом магнитной системой. В витках катушки, пересекающих магнитные силовые линии, возникает напряжение, являющееся выходным сигналом микрофона.

Электростатический (конденсаторный) микрофон представляет собой конденсатор, состоящий из двух пластин, разделенных слоем диэлектрика. Одна из пластин является мембраной, которая может колебаться под действием звукового давления относительно второй неподвижной пластины. При колебаниях мембраны емкость конденсатора изменяется счастотой воздействующего на мембрану звукового давления. Вследствие этого в электрической цени появляется переменный ток той же частоты и возникает падение напряжения нанагрузочном сопротивлении, являющееся выходным напряжением микрофона.

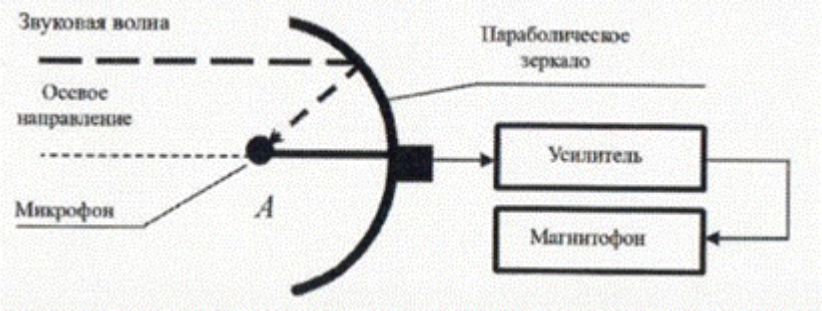
Действие **пьезоэлектрических электроакустических преобразователей** основано на проявлении пьезоэлектрического эффекта, т.е. на возникновении поляризации диэлектрика при механическом воздействии на него. Этот эффект наблюдается в кристаллах кварца, в сегнетоэлектриках и в некоторых других материалах. В пьезоэлектрическом микрофоне звуковоедавление воздействует непосредственно или через диафрагму и соединенный с ней стержень на пьезоэлектрический элемент (кристалл, пьезокерамику). При деформации последнего на егообкладках вследствие пьезоэлектрического эффекта возникает напряжение, являющееся выходным сигналом микрофона.

Виды направленных микрофонов:

- Параболические
- Плоские акустические фазированные решетки
- Трубчатые
- Градиентные

Параболический микрофон.

Параболическая акустическая антенна представляет собой параболическое зеркало диаметром 20–50 см, в фокусе которого размещается мембрана микрофона.



Плоская фазированная решетка обеспечивает одновременный прием звукового поля в дискретных точках некоторой плоскости, перпендикулярной к направлению на источник звука. В этих точках размещаются либо микрофоны с суммированием сигналов электрическим способом, либо открытые торцы звуководов, которые обеспечивают синфазное сложение звуковых пален от источника в акустическом сумматоре.

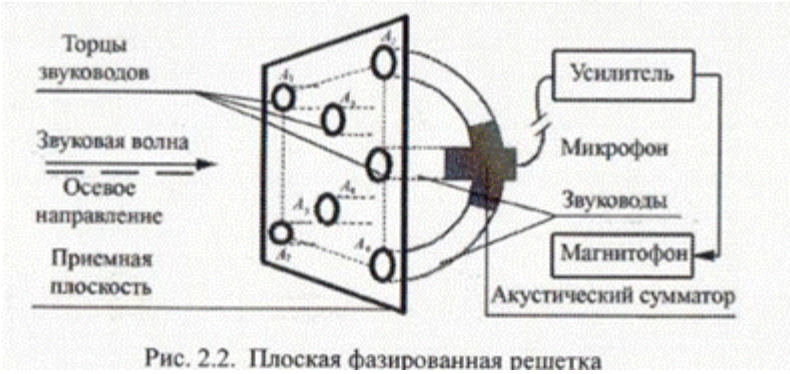


Рис. 2.2. Плоская фазированная решетка

Трубчатый остронаправленный микрофон состоит из одной трубки длиной 0.3–1 м или набора трубок, длины которых согласованы с длинами волн акустического сигнала. В торце трубок укрепляется мембрана микрофона.

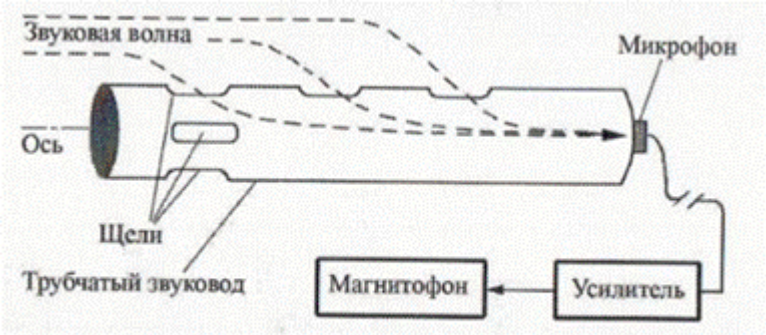


Рис. 2.3. Трубчатый микрофон

Градиентный микрофон основан на операции вычитания акустических сигналов по направлению прихода сигнала.

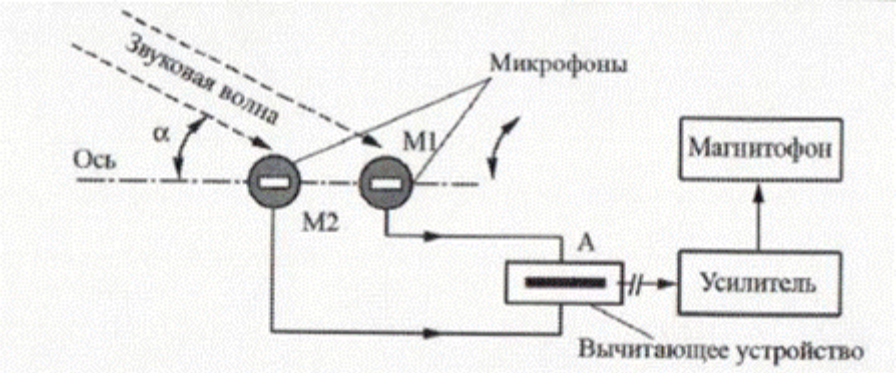


Рис. 2.4. Простейший градиентный микрофон

По диапазону частот микрофоны разделяются на узкополосные и широкополосные. Узкополосные микрофоны предназначены для передачи речи. Широкополосные микрофоны имеют более широкую полосу частот и преобразуют колебания в звуковом и частично ультразвуковом диапазонах частот.

По способу применения микрофоны разделяются на воздушные, гидроакустические (гидрофоны) и контактные. Контактные микрофоны предназначены для приема структурного звука.Например, контактный стетоскопный микрофон UM–012, прикрепленный к стене помещения, позволяет прослушивать разговоры в соседнем помещении при толщине стен до 50 см.Модификацией контактных микрофонов являются ларингофоны и остеофоны, воспринимающие и преобразующие в электрические сигналы механические колебания (вибрации) связок и хрящей гортани или кости черепа говорящего.

С целью обеспечения реальной возможностью скрытного подслушивания и существенного повышения его дальности широко применяются **закладные устройства** (закладки, радио-микрофоны, «жучки», «клопы»). По виду носителя информации от закладных устройств к злоумышленнику их можно разделить на проводные и излучающие закладные устройства.Проводные акустические закладки в виде микрофона имеют высокую чувствительность и помехоустойчивость, но наличие провода демаскирует закладки и усложняет их установку, в особенности в условиях дефицита времени. Излучающие закладные устройства лишены недостатков проводных, но у них проявляется другой демаскирующий признак – излучения в радио- иоптическом диапазонах.

Для более 96% радиозакладок рабочие частоты сосредоточены в интервале 88–501 МГц, причем с частотами 92.5–169.1 МГц выпускаются 42% радиомикрофонов, а с частотами 373.4–475.5МГц – 52% радиомикрофонов [5, 16]. Наиболее интенсивно используется диапазон частот 449.7–475.5 МГц, в котором сосредоточены рабочие частоты 36% образцов.

Литература: Титов, А. А. Технические средства защиты информации : учебное пособие / А. А. Титов. – Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. – 194 с.; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=208661

Лекция 7. Классификация и структура технических каналов утечки информации

Тезисы лекции:

- Типовая структура и виды технических каналов утечки информации.
- Каналы утечки речевой информации.
- Каналы утечки информации при её передаче по каналам связи.
- Каналы утечки видовой информации.

- Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.
- Каналы утечки информации за счет побочных электромагнитных излучений и наводок.

Слайды презентации к лекции:





КЛАССИФИКАЦИЯ КАНАЛОВ



3

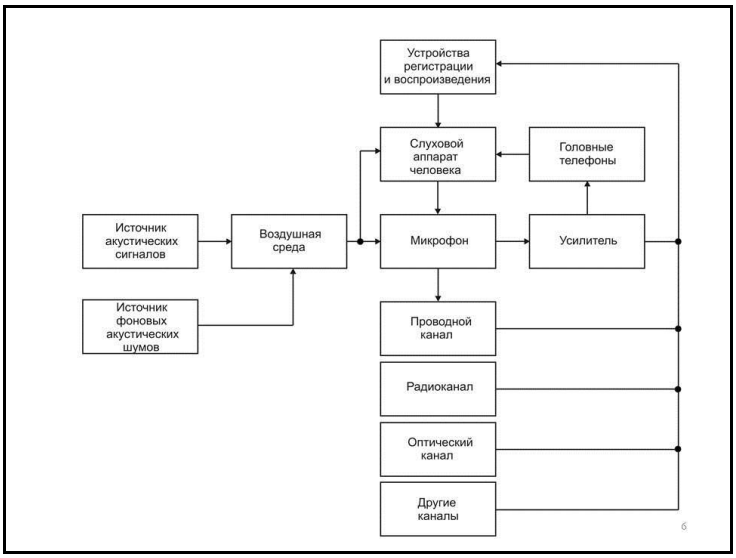
Прямой акустический канал

Наиболее простым способом перехвата речевой информации является подслушивание (прямой перехват). Акустические сигналы могут непосредственно приниматься ухом человека, реагирующим на изменение звукового давления, возникающего при распространении звуковой волны в окружающем пространстве. Диапазон частот акустических колебаний, слышимых человеком, от 16-25 Гц до 18-20 кГц в зависимости от индивидуальных особенностей слушателя. Человек воспринимает звук в очень широком диапазоне **звуковых давлений**, одной из базовых величин этого диапазона является **стандартный порог слышимости**. Под ним условились понимать эффективное значение звукового давления, создаваемого гармоническим звуковым колебанием частотой F=1000 Гц, едва слышимым человеком со средней чувствительностью слуха. Порогу слышимости соответствует звуковое давление $P=2\cdot10^{-5}$ Па. Верхний предел определяется значением P=20 Па, при котором наступает болевое ощущение.

4

- В случаях, когда уровни звукового давления, создаваемого звуковой волной, ниже порога слышимости, когда нет возможности непосредственно прослушивать речевые сообщения или требуется их зафиксировать (записать), используют микрофон.
- Микрофон является преобразователем акустических колебаний в электрические сигналы. К микрофонам, используемым в технике акустической разведки, предъявляют высокие требования. Необходимо обеспечить высокую разборчивость и узнаваемость речевого сигнала. Кроме того, микрофоны должны обладать направленными свойствами, высокой чувствительностью и малыми габаритами.
- При необходимости передать перехваченное речевое сообщение на расстояние используют проводные, оптические, радио- и другие каналы. В этих случаях используемые устройства называются закладными устройствами для перехвата акустической информации. В состав радиозакладки может быть включено запоминающее устройство.

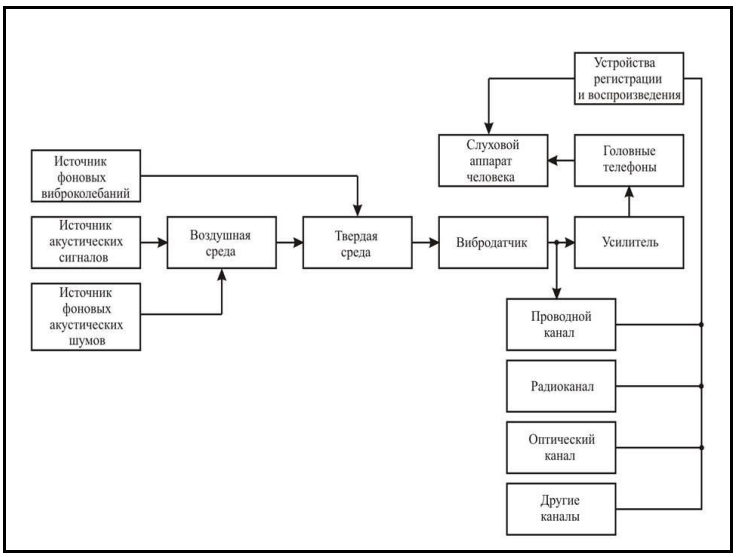
5



Виброакустический канал

Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, в результате виброакустичесого преобразования, возникают вибрационные колебания.
Средой распространения сигналов являются ограждающие строительные конструкции помещений (стены, потолки, полы) и инженерные коммуникации (трубы водоснабжения, отопления, вентиляции и т.п.).
Для перехвата речевых сигналов в этом случае используются вибродатчики (акселерометры). Сигнал, снимаемый с выхода вибродатчика, после усиления может быть прослушен, зарегистрирован на магнитном или другом носителе или передан в пункт приема, находящийся на удалении от места прослушивания, по проводному, радио- или иному передачи информации

7

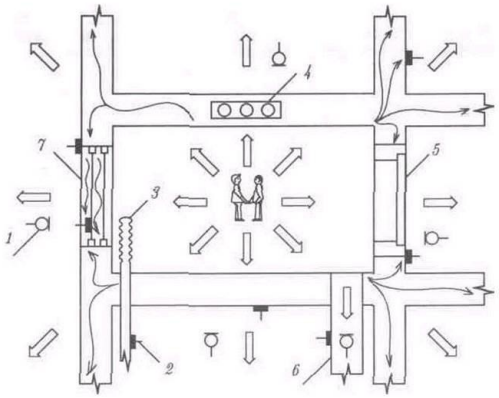


В целях ведения разведки с использованием виброакустического канала широко применяются стетоскопы, т.е. устройства, содержащие вибродатчик (стетоскопный микрофон), блок обработки сигнала, осуществляющий его усиление и ослабление помех, и головные телефоны.
Необходимо отметить, что чем тверже материал преграды на пути распространения акустических колебаний, тем лучше он передает вибрации, вызываемые ими. Вибродатчик обычно крепится к металлическому предмету, вмонтированному в стену. В качестве звукопровода могут использоваться трубы водоснабжения, канализации, батареи отопления и т.д.
Когда нет возможности разместить пункт прослушивания в непосредственной близости от места установки вибродатчика (стетоскопа), в состав аппаратуры прослушивания включают проводные, радио- и другие каналы передачи информации, аналогичные каналам, используемым в закладных устройствах.

9

Схема акустических каналов утечки информации

•Схема акустических и виброакустических каналов утечки информации в помещении:
1 – микрофон подслушивания;
2 – вибродатчики подслушивания;
3 – батарея
• отопления;
4 – полость для кабелей;
5 – дверь;
6 – воздушные вентиляции;
7 – окно



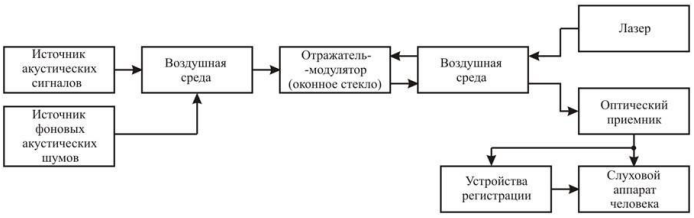
Если акустические и вибрационные датчики установлены на этих конструкциях за пределами помещения, это дает возможность принять речевые сигналы и проконтролировать разговоры внутри него. При этом необязательно скрытно проникать в помещение. Установить датчик можно и с помощью специальных выстреливающих устройств (например на оконную раму). Иногда используют лазерные устройства и направленные микрофоны.

11

Акустооптический канал

Перехват речевой информации из помещений может осуществляться с помощью лазерных средств акустической разведки. В этом случае применяется дистанционное лазерно-локационное зондирование объектов, являющихся потенциальными источниками конфиденциальной речевой информации. В качестве таких объектов могут выступать оконные стекла и другие виброотражающие поверхности.
Генерируемое лазерным передатчиком колебание наводится на оконное стекло помещения. Возникающие при разговоре акустические волны, распространяясь в воздушной среде, воздействуют на оконное стекло и вызывают его колебания. Таким образом, происходит виброакустическое преобразование речевого сообщения. Лазерное излучение, падающее на внешнюю поверхность оконного стекла (мембраны), в результате вибро-оптического преобразования оказывается промодулированным сигналом, вызывающим колебания мембраны. Отраженный оптический сигнал принимается оптическим приемником, в котором осуществляется восстановление сообщения.

12



К настоящему времени созданы различные системы лазерных средств акустической разведки, имеющие дальность действия от десятков метров до единиц километров. Наведение лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира.

13

Акустоэлектрический канал

Возникают за счет преобразований акустических сигналов в электрические.
Некоторые элементы вспомогательных технических средств и систем (ВТСС), в том числе трансформаторы, катушки индуктивности, звонков телефонных аппаратов и т.п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), либо к модуляции токов, протекающих по этим элементам в соответствии с изменениями воздействующего акустического поля.
ВТСС, кроме указанных элементов, могут содержать непосредственно акустоэлектрические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т.д.

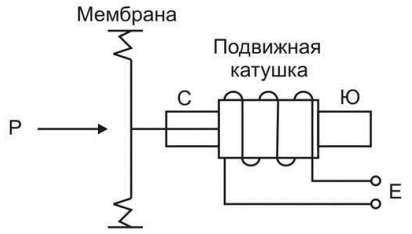
14

Индуктивные акустоэлектрические преобразователи

Если в поле постоянного магнита поместить катушку индуктивности (рамку) и вращать ее хотя бы под воздействием воздушного потока, то на ее выходе появится ЭДС индукции.
Воздушный поток переменной плотности возникает и при разговоре человека. Поэтому в соответствии с разговором (под воздействием его воздушного потока) будет вращаться катушка (рамка), что вызовет пропорционально изменяющуюся ЭДС индукции на ее концах. Таким образом, можно связать акустическое воздействие на провод в магнитном поле с возникающей ЭДС индукции на его концах - это типичный пример из группы индукционных акустических преобразователей. Представителем этой группы является, например, электродинамический преобразователь.

15

ЭДС зависит от вектора магнитной индукции, магнитной проницаемости сердечника, угла между вектором и осью катушки, угла между вектором и осью сердечника и площадей поперечных сечений сердечника и катушки. Индуктивные преобразователи подразделяются на электромагнитные, электродинамические и магнитострикционные. Примером непосредственного использования этого эффекта для целей акустического преобразования является электродинамический микрофон



17

Электромеханический вызывной звонок телефонного аппарата — типичный представитель индуктивного акустоэлектрического преобразователя, микрофонный эффект которого проявляется при положенной микротелефонной трубке.

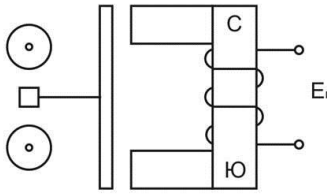


Схема вызывного звонка

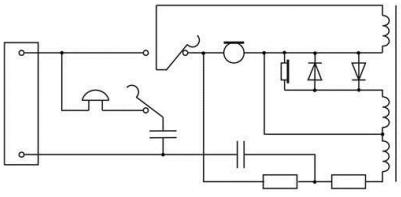


Схема телефонного аппарата

19

На таком же принципе (электромеханического вызывного звонка) образуется микрофонный эффект и в отдельных типах электромеханических реле различного назначения Акустические колебания воздействуют на якорь реле. Колебания якоря изменяют магнитный поток реле, замыкающийся по воздуху, что приводит к появлению на выходе катушки реле ЭДС микрофонного эффекта.

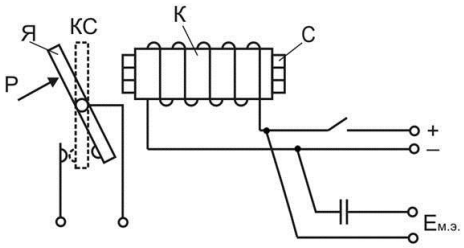
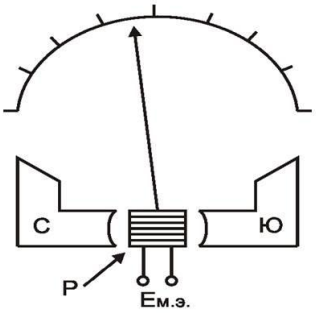


Схема работы реле: КС — контактная система; К — катушка; С - сердечник

21

В магнитоэлектрическом измерительном приборе имеются неподвижный постоянный магнит и подвижная рамка, которая поворачивается вокруг своей оси под воздействием собственного магнитного поля, создаваемого измеряемым напряжением, и магнитного поля постоянного магнита.



Если акустические колебания воздействуют на рамку, она вращается под их давлением и на ее концах возникает ЭДС индукции.

Практически аналогичная ситуация будет при воздействии акустических колебаний на электромагнитный измерительный прибор.

Устройство магнитоэлектрического измерительного прибора

Представителем индукционных акустоэлектрических преобразователей являются трансформаторы.

Акустическое влияние на сердечник и обмотку трансформатора приведет к появлению микрофонного эффекта. Если ЭДС индукции появляется в первичной обмотке, то во вторичной обмотке она увеличивается на значение коэффициента трансформации.

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

Обратное по отношению к магнитострикции явление — Виллари-эффект (изменение намагничиваемости тела при его деформации). В усилителях с очень большим коэффициентом усиления входной трансформатор на ферритах при определенных условиях вследствие магнитострикционного эффекта способен преобразовывать механические колебания в электрические.

24

Емкостные преобразователи

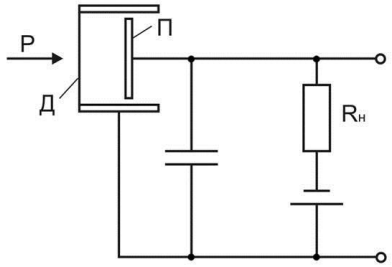
Емкостные преобразовывающие элементы превращают изменение емкости в изменение электрического потенциала, тока, напряжения.

емкость конденсатора

зависит от расстояния между пластинами. Воздействующее на пластины акустическое давление, изменяя расстояние между пластинами, приводит к изменению емкости. Изменение емкости приводит к изменению сопротивления цепи и соответственно, к падению напряжения на сопротивлении нагрузки пропорционально акустическому давлению. Эти зависимости используются в конструкции конденсаторных микрофонов.

25

Когда на микрофон действует волна звукового давления Р, диафрагма Д движется относительно неподвижного электрода — жесткой пластины П. Это движение вызывает переменное изменение электрической емкости между диафрагмой и задней пластиной, а следовательно, производит соответствующий электрический сигнал на выходе.



Устройство конденсаторного микрофона

26

Параметрический канал

В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов технических средств передачи информации, что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом.

Параметрический канал утечки информации может быть реализован и путем “высокочастотного облучения” помещения, где установлены закладные устройства, параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются под действием акустического (речевого) сигнала.

29

Электрический канал

Возникает за счет наводок электромагнитных излучений технических средств, обрабатывающих конфиденциальную информацию на соединительные линии и посторонние проводники, выходящие за пределы контролируемой зоны; а также за счет паразитных связей между информационными и посторонними цепями.

Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ТСПИ и посторонних проводников.

32

Индукционный канал

Используется эффект возникновения вокруг электрических цепей электромагнитного поля при прохождении по ним информационных электрических сигналов, которые перехватываются специальными индукционными датчиками.

Индукционные датчики применяются в основном для съема информации с симметричных высокочастотных кабелей.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабженные магнитными антеннами.

33

Паразитные связи и наводки

Элементы, цепи, тракты, соединительные провода и линии связи любых электронных систем и схем постоянно находятся под воздействием собственных (внутренних) и сторонних (внешних) электромагнитных полей различного происхождения, индуцирующих или наводящих в них значительные напряжения. Такое воздействие называют электромагнитным влиянием, или просто влиянием на элементы цепи. Так как такое влияние образуется непредусмотренными связями, то говорят о паразитных (вредных) связях и наводках, которые также могут привести к образованию каналов утечки информации.

Основными видами паразитных связей в схемах электромагнитных устройств являются емкостные, индуктивные, электромагнитные, электромеханические и связи через источники питания и заземления радиоэлектронных средств. Рассмотрим паразитные связи и наводки на примере широко распространенных усилительных схем различного назначения.

34

Паразитные емкостные связи

Эти связи обусловлены наличием электрической емкости между элементами, деталями и проводниками усилителей, несущих потенциал сигнала. Так как сопротивление емкости, создающей паразитную емкостную связь, падает с ростом частоты, проходящая через нее энергия с повышением частоты увеличивается. Поэтому паразитная емкостная связь может привести к самовозбуждению на частотах, превышающих высшую рабочую частоту усилителя.

Чем больше усиление сигнала между цепями и каскадами, имеющими емкостную связь, тем меньшей емкости достаточно для его самовозбуждения. При усилении в 10^5 раз (100 дБ) для самовозбуждения усилителя звуковых частот иногда достаточно емкости между входной и выходной цепями $C_{пс} = 0{,}01$ пФ.

35

Индуктивные связи

Такие связи обусловлены наличием взаимоиндукции между проводниками и деталями усилителя, главным образом, между его трансформаторами. Паразитная индуктивная обратная связь между трансформаторами усилителя, например между входным и выходным трансформаторами, может вызвать самовозбуждение в области рабочих частот и на гармониках.

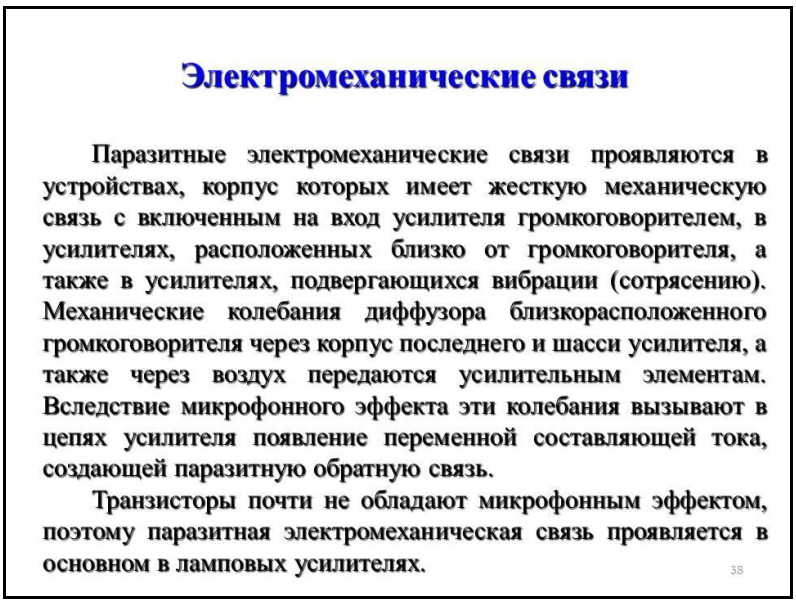
Для усилителей с малым входным напряжением очень опасна индуктивная связь входного трансформатора с трансформаторами питания. Значительно слабее паразитная индуктивная связь проявляется при тороидальной конструкции входного трансформатора. Паразитная индуктивная связь ослабляется при уменьшении размеров трансформаторов.

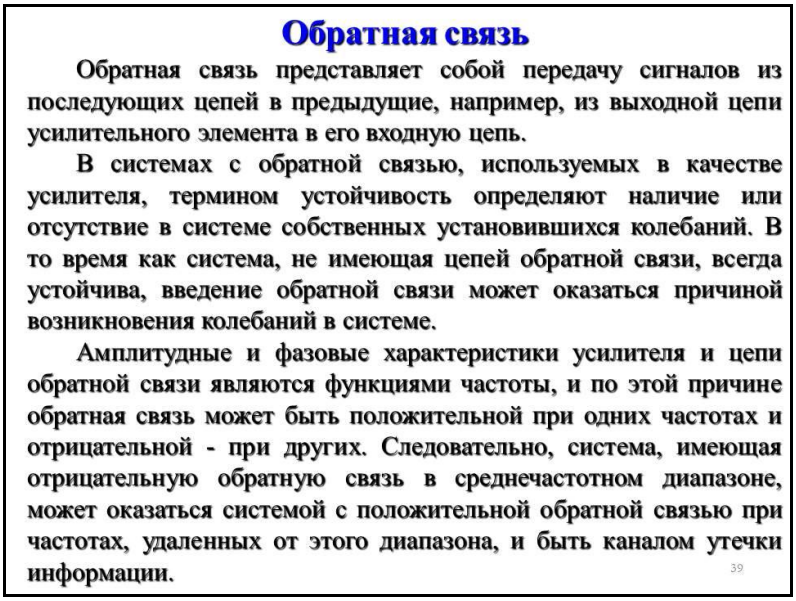
36

Электромагнитные связи

Паразитные электромагнитные связи приводят к самовозбуждению отдельных каскадов звуковых и широкополосных усилителей на частотах порядка десятков и сотен мегагерц. Эти связи обычно возникают между выводными проводниками усилительных элементов, образующими колебательную систему с распределенными параметрами на резонансной частоте определенного значения.

37





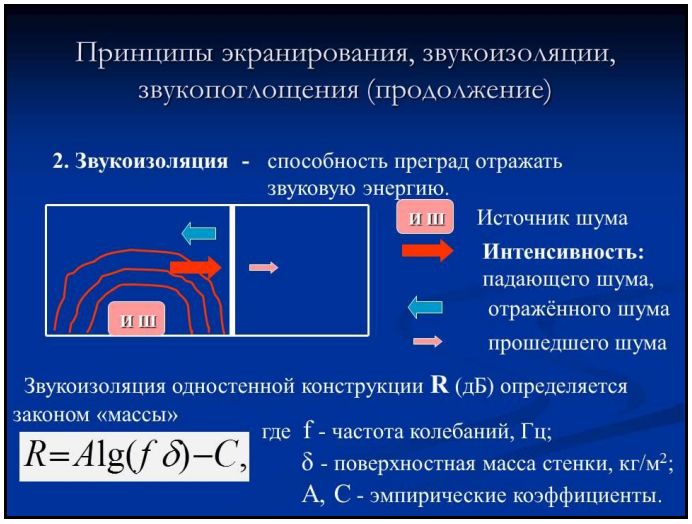
Литература: Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. – 7-е изд., испр. – Москва : Горячая линия – Телеком, 2012. – 442 с. : ил. – ISBN 978-5-9912-0233-6; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=253208

Лекция 8. Средства предотвращения утечки информации по техническим каналам
Тезисы лекции:

- Средства маскировки и дезинформирования в оптическом и радиодиапазонах.
- Средства звукоизоляции из звукопоглощения.
- Средства обнаружения, локализации и подавления сигналов закладных устройств.
- Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.
- Генераторы линейного и пространственного зашумления.

Иллюстративный материал к лекции:







Конструктивные средства уменьшения шума

Для уменьшения аэродинамического шума систем вентиляции, шума газотурбонаддува и газовыхлопа двигателей применяют реактивные (рис.21, а) и активные (рис.21, б) глушители.



Рис. 21

Расширительная камера Глушитель со звукопоглотителем

Звукоизоляция источника шума обеспечивается кожухом (рис.22 а), а звукоизоляция рабочего места - изолированной кабиной (рис.22 б)

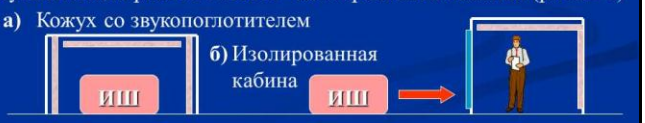


Рис. 22

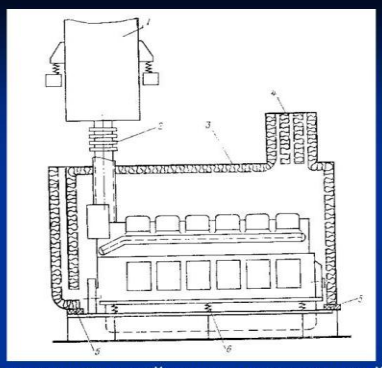


Рис. 23 Звукоизолирующий кожух, установленный на дизель.

1 - глушитель газовыхлопа; 2 - компенсатор; 3 - звукопоглотитель; 4 - глушитель воздухоприёма; 5 - резина; 6 - виброизоляторы.

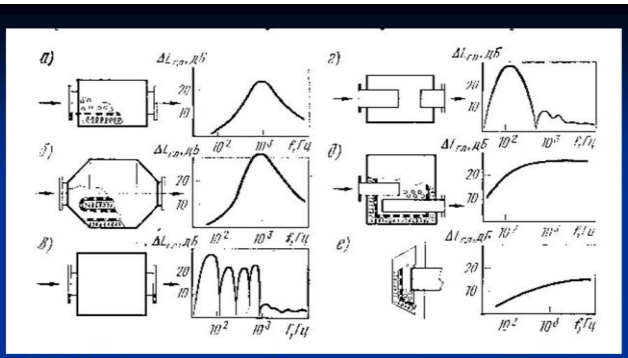


Рис. 24 Типы глушителей шума и характер заглушаемого ими спектра.

а - звукопоглощающий патрубок; б - пластинчатый; в - камерный; г - камерный с трубами внутри; д - камерный несоосный со звукопоглотителем; е - экранный.

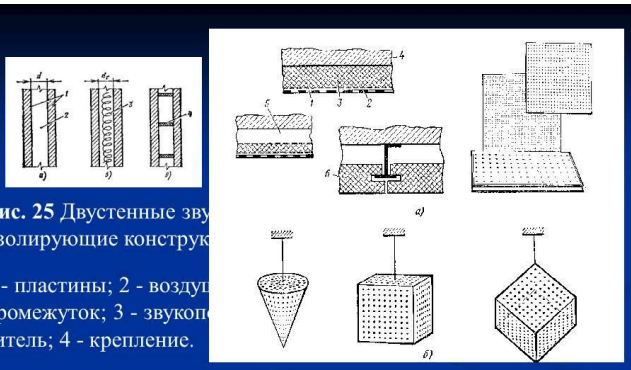


Рис. 25 Двустенные зву
изолирующие конструк

1 - пластины; 2 - воздуш
промежуток; 3 - звукопо
титель; 4 - крепление.

Рис. 26 Звукопоглощающие конструкции
1 - защитный перфорированный экран; 2 - стеклоткань; 3 - звукопоглощающий материал; 4 - стена или потолок; 5 - воздушный промежуток; 6 - плита из звукопоглощающего материала.

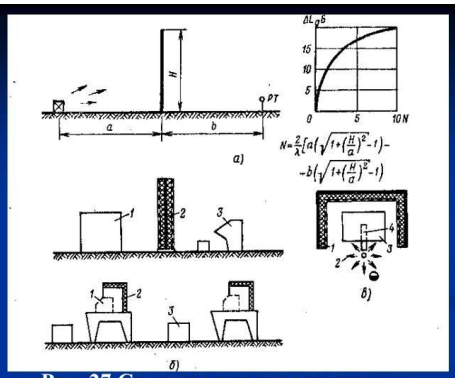


Рис. 27 Средства экранирования
а - схема экрана; б - экранирование нескольких источников шума; в - экранирование источников механического шума; 1 - оборудование; 2 - экран со звукопоглотителем; 3 - рабочее место; 4 - дисковая пила.

Классификация обнаружителей радиоизлучений закладных устройств



Классификация средств обнаружения неизлучающих закладок



Классификация средств подавления закладных устройств



Противодействие перехвату речевой информации

* Информационное скрытие
* Энергетическое скрытие
* Обнаружение, локализация и изъятие закладных устройств


Способы подавления опасных электрических сигналов
Способы подавления опасных сигналов
Пассивные
Активные
Отключение источников опасных сигналов
Фильтрация опасных сигналов
Ограничение опасных сигналов
Применение буферных устройств
Линейное зашумление
Пространственное зашумление


СЗИ от утечки по ТКУИ
Система «Барон»
Соната
Комплекс для проведения акустических и виброакустических измерений СПРУТ-7А
"Копейка" вибрационный излучатель на стекло
"Молот" вибрационный излучатель на стену
Вибропреобразователь на оконное стекло КВП-7
Вибропреобразователь на стену КВП-2
"Серп" вибрационный излучатель на раму окна
Акустический преобразователь на дверной проём
Система «Шорох-2М»


СЗИ от утечки по ТКУИ
Акустический сейф "Ладья"
Нелинейный локатор
«МОРФЕЙ-МК» предназначен для блокирования возможности организации связи между базовыми станциями (дальность подавления до 50 метров)
Эндоскоп, зеркала





Литература: Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. – 7-е изд., испр. – Москва : Горячая линия – Телеком, 2012. – 442 с. : ил. – ISBN 978-5-9912-0233-6; То же [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=253208

Лекция 9. Итоговая лекция. Подведение и анализ промежуточных результатов освоения дисциплины

Итоговая лекция завершает изучение дисциплины, обобщает пройденное за весь период. При ее подготовке учитываются пробелы в знаниях аспирантов, выявленные на практических занятиях и при оценке самостоятельной работы. Аспиранты получают установку на их устранение и на дальнейшее совершенствование своей подготовки в данной области. На лекции подводятся итоги изучения дисциплины, показывается ее значение в профессиональной сфере и формировании научного мировоззрения, обсуждается вопрос о подведении итогов изучения дисциплины – сдаче зачета или экзамена.

2. Методические указания по подготовке к занятиям семинарского типа

2.1. Планы и (или) методические рекомендации к практическим занятиям

В рамках проведения занятий по дисциплине предполагается организация следующих практических занятий:

Практическое занятие 1. Основные концептуальные положения инженерно-технической защиты информации

Тематика: Показатели эффективности инженерно-технической защиты информации.

Текст задания:

Цель работы: Приобрести практические навыки в определении степени защищенности объекта информатизации путем моделирования возможных действий технических разведок. Научиться определять потенциальные и реальные каналы утечки информации.

Теоретическая часть:

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить потенциальные и реальные угрозы технического проникновения на защищаемый объект, возможные каналы для несанкционированного доступа и утечки защищаемой информации.

Данная работа базируется на знании природы возникновения технических каналов утечки информации и методов ведения технической разведки. Правильное определение потенциальных угроз на предпроектном этапе построения системы защиты позволит в дальнейшем выбрать наиболее оптимальные меры и средства защиты.

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

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и др. Наибольшее внимание следует уделить вспомогательным средствам, имеющие линии, выходящие за пределы контролируемой зоны.

В качестве каналов утечки больше внимания следует уделить вспомогательным средствам, имеющим линии, выходящие за пределы контролируемой зоны, а также посторонним проводам и кабелям, проходящим через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

При оценке защищенности помещений от утечки речевой информации необходимо учитывать возможность ее прослушивания как из соседних помещений, так и с улицы. Следует проводить оценку возможности ведения разведки с использованием лазерных микрофонов. Интерес могут вызывать каналы утечки за счет вибраций, возникающих под давлением акустических волн, в твердых телах (ограждениях, трубах и т.п.).

Оценка защищенности объекта включает в себя анализ режима работы и охраны объекта, с целью моделирования действий по скрытному проникновению на них (неконтролируемому пребыванию) посторонних лиц. Режим работы специалистов сторонних организаций, приобретение, установка и ремонт мебели, оргтехники и т.п. Т.е. всю совокупность условий, позволяющих внедрить на объект специальные закладные устройства перехвата информации (микропередатчики, возможность установки миниатюрных микрофонов с подключением к внешним линиям и т.д.). А также определение наиболее эффективных, для использования на разных уровнях проникновения, средств технической разведки.

Большое, а иногда решающее, значение при оценке угрозы может иметь знание наиболее вероятного противника, его финансовых и оперативных возможностей, знание личностных качеств постоянного персонала, временных работников и другая дополнительная информация.

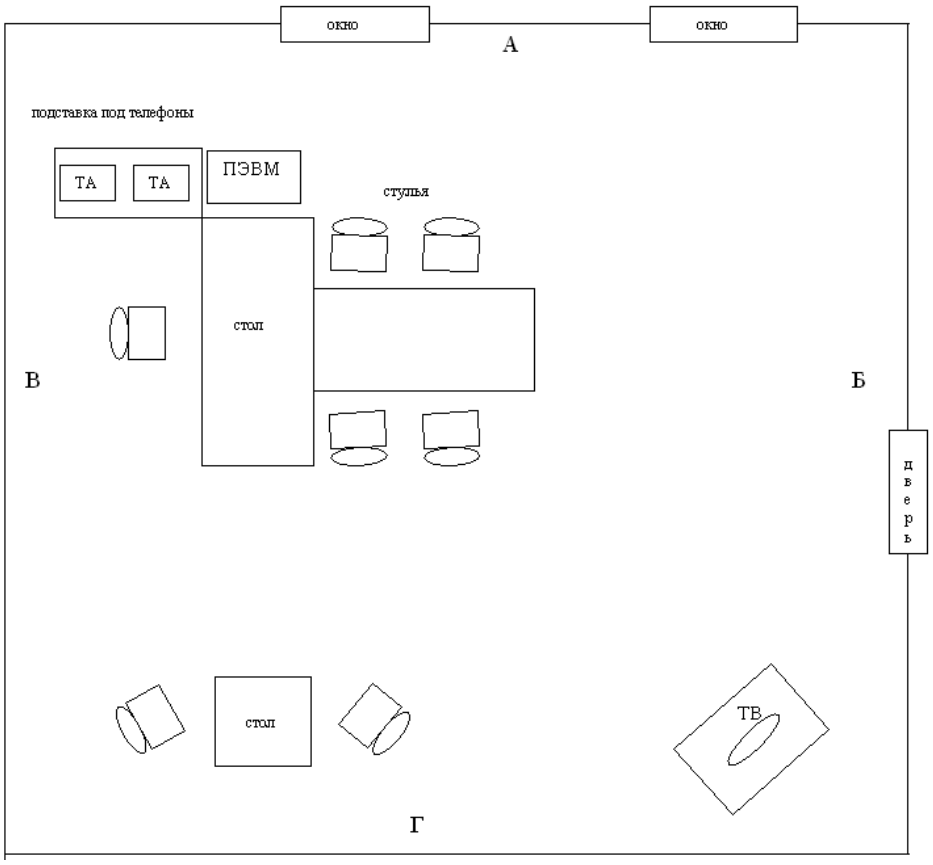
Определение потенциальных и реальных ТКУИ:

Ниже приведена примерная характеристика защищаемого объекта (исходные данные).

1. Защищаемое помещение расположено на четвертом этаже 7-этажного здания. Все здание принадлежит одной организации:
   - Сверху расположены служебные помещения.
   - Снизу расположены технические помещения (туалет, электрощитовая).
   - Со стороны стены Б расположена приемная.
   - Со стороны стены Г расположен общий коридор.

   Стороны А и В выходят на улицы с интенсивным пешеходным и транспортным движением.

   Окна помещения оборудованы шторами, смотрят на жилой дом расположенный на расстоянии 30 метров.
2. Из мебели в помещении установлены рабочий и журнальный столы, стулья, подставки под: телефоны, ПЭВМ и телевизор.
3. Из основных технических средств в помещении установлен телефон внутренней конфиденциальной связи, ПЭВМ включенная в локальную сеть.
4. Из вспомогательных технических средств в помещении установлен телефон ГТС, телевизор, радиотрансляционный приемник. Помещение оборудовано системой пожарной и охранной сигнализации, линии которых выходят на пульт дежурного охранника. Помещение электрифицировано (освещение, питание оборудования).
5. Помещение оборудовано системой вытяжной вентиляции, короб которой проложен вдоль коридора и поднимается на крышу здания. Радиаторы отопления установлены вдоль стены А. Трубы отопления спускаются в подвал.
6. Режим работы учреждения предусматривает свободное передвижение сотрудников и посетителей в рабочее время. В ночное время помещение закрывается на ключ, сдается под охрану дежурному. Системы связи обслуживаются штатным сотрудником. Системы жизнеобеспечения (отопление, канализация) обслуживаются по заявке приходящим сотрудником.
7. Доступ штатных сотрудников к служебной информации не разграничен.



В качестве примера представим порядок рассуждения защищенности объекта со стороны окон. При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допущено использование оговорок типа " если.... то....".

1. Просмотр помещения со стороны улицы, ввиду того, что помещение находится на 4 этаже, не возможен. Так как возможен просмотр помещения извне, со стороны жилого дома с помощью оптических приборов, существует потенциальный канал утечки видовой информации.
   Однако, если организационными мероприятиями (соответствующим инструктажем ответственных лиц) введено обязательное зашторивание окон во время проведением совещаний, работы с документами и т.п., то реального визуально оптического канала утечки информации нет.
   В качестве дополнительных мер можно ввести периодический контроль за соблюдением сотрудниками правила зашторивания, а также поставить тонированные или рифленые стекла.
2. Так как возможно прослушивание помещения, со стороны улицы и жилого дома, через открытые окна и форточки с помощью направленных микрофонов, существует потенциальный канал утечки акустический информации.
   Однако, если организационными мероприятиями введено обязательное закрытие окон и форточек во время проведения совещаний, реального акустического канала утечки информации нет.
   В качестве дополнительной меры можно установить кондиционер или приобрести генератор белого шума и включать его во время проведения совещаний.
3. Так как возможен съем информации о ведущихся в помещении разговорах с оконных стекол, за счет их вибрации, при использовании лазерного микрофона, при расположении

поста перехвата в жилом доме, существует еще один потенциальный канал утечки акустической информации.

В данном случае с помощью одних организационных мероприятий устранить канал утечки не представляется возможным. Однако реальное существование канала утечки может быть констатировано лишь после проведения инструментальных измерений.

По результатам инструментальной проверки будет определяться необходимость проведение защитного мероприятия, например установка рифленых стекол или зашумление стекол и пространства между ними.

В заключение первого этапа можно предложить установку стекол с рифленой поверхностью и кондиционера. Решение представляется оптимальным, т.к. акустический и визуально оптический каналы устраняются при минимальных финансовых затратах. Также, в дальнейшем, обеспечивается удобство эксплуатации объекта и исключается негативный человеческий фактор.

При оценке вероятности использования технической разведкой потенциальных каналов утечки информации следует принимать во внимание окружающую обстановку, с точки зрения возможности по организации и ведению технической разведки, а именно:

- скрытное размещение поста перехвата (для прослушивания и просмотра помещения) на улице с интенсивным движением затруднительно, т.к. подозрительные лица, транспортные средства и т.п. привлекают к себе внимание, легко визуально обнаруживаются;
- скрытное размещение поста перехвата (для прослушивания и просмотра помещения, установки лазерного микрофона) в жилом здании, если, например, арендовать квартиру с окнами расположенными напротив окон защищаемого помещения, вполне реализуемо.

Необходимо, если имеется такая возможность, проверить благонадежность (лояльность) жильцов в квартирах, потенциально пригодных для организации поста перехвата (сдаются ли квартиры, проживают ли в квартирах потенциальные конкуренты, имеются ли лица бывшие в конфликте с законом и т.п.). Возможности организации постов перехвата на технических этажах и т.п.

В случае получения в ходе проверки положительных данных можно заключить, что защитные мероприятия не требуются вообще. С точки зрения защиты от случайных утечек, например прослушивания, можно заключить, что улица с интенсивным автомобильным и пешеходным движением создает достаточно сильную акустическую помеху, за которой разговоры случайными прохожими различаться не будут. При необходимости в этом можно убедиться экспериментально.

В случае получения в ходе проверки отрицательных или неоднозначных данных оптимальным остается вариант указанный в заключение первого этапа.

Самостоятельная часть работы: В самостоятельной части работы предлагается:

- выявить оставшиеся, потенциально возможные каналы утечки информации (с учетом исходных данных, используя, при необходимости оговорки);
- смоделировать возможные действия технических разведок, определить реальные каналы утечки информации;
- доказать целесообразность и предложить проведение тех или иных защитных мероприятий.

Примечание: При определении вероятности существования каналов утечки, в случае недостаточности исходных данных, допускается использовать оговорку типа " если.... то....".

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если работа выполнена полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 2. Виды информации, защищаемой техническими средствами

Тематика: Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.

Текст задания: Найдите ответы на предложенные ниже вопросы, используя возможности поисковых систем.

1. Что понимают под предметом защиты? Под объектом защиты? Дайте их классификацию.
2. Дайте классификацию АС, обрабатывающих КИ.
3. Перечислите исходные данные и определяющие признаки для классификации АС.
4. Дайте характеристику классов защищённости АС от НСД к информации.
5. Перечислите подсистемы для обеспечения защиты от НСД.
6. Назовите классы защищённости СВТ от НСД. Какие требования к ним предъявляются?
7. Перечислите виды угроз реализуемых по сети.
8. Перечислите наиболее распространенные атаки в сетях, способы их ослабления и контрмеры.
9. Что такое контрольно-пропускной режим?
10. Назовите программно-технические средства СКУД.
11. Дайте классификацию устройств идентификации доступа.
12. В чем отличие идентификации от верификации в биометрических СКУД?

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;

Оценка «хорошо» выставляется, если аспирант ошибся при ответе на один-два вопроса;

Оценка «удовлетворительно» выставляется, если аспирант ошибся при ответе на три-четыре вопроса.

Оценка «неудовлетворительно» выставляется, если аспирант допустил больше четырех ошибок.

Практическое занятие 3. Демаскирующие признаки объектов защиты

Тематика:

- Классификация демаскирующих признаков.
- Опознавательные признаки и признаки деятельности.
- Видовые демаскирующие признаки.
- Демаскирующие признаки сигналов.
- Демаскирующие признаки веществ.
- Именные, прямые и косвенные демаскирующие признаки.

Текст задания: Составить тест по теме «Демаскирующие признаки объектов защиты». Вопросы должны отображать содержание всех изученных тем. Количество вопросов – не менее 30. Тест может быть создан в любом программном средстве (например, MyTestX), либо онлайн-сервисе (Яндекс.Формы).

Шкала оценивания:

Оценка «отлично» выставляется за практическую работу, если представленный тест отражает содержание более 80% изученного материала;

Оценка «хорошо» выставляется за практическую работу, если представленный тест отражает содержание более 60% изученного материала;

Оценка «удовлетворительно» выставляется за практическую работу, если представленный тест отражает содержание более 40% изученного материала.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена или тест отражает содержание менее 40% изученного материала.

Практическое занятие 4. Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей

Тематика: Виды источников и носителей информации.

Текст задания: Найдите ответы на предложенные ниже вопросы, используя возможности поисковых систем.

1. Что такое носитель информации?
2. Какой носитель информации чаще всего использует человек?
3. Приведите примеры искусственных носителей информации.
4. Приведите примеры естественных носителей информации.
5. Кто (или что) может быть носителем информации?
6. Кто (или что) может быть приемником информации?
7. Дайте характеристику классов понятий риск и ущерб.
8. Охарактеризуйте способы количественной и качественной оценки рисков.
9. В каком законе приведена классификация средств защиты информации?
10. Назовите основные положения Доктрины информационной безопасности РФ.
11. Что представляет собой программно-математическое воздействие на информацию?
12. Что представляет собой математическая модель воздействия нарушителей?

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;

Оценка «хорошо» выставляется, если аспирант ошибся при ответе на один-два вопроса;

Оценка «удовлетворительно» выставляется, если аспирант ошибся при ответе на три-четыре вопроса.

Оценка «неудовлетворительно» выставляется, если аспирант допустил больше четырех ошибок.

Практическое занятие 5. Виды угроз безопасности информации, защищаемой техническими средствами

Тематика: Технические каналы утечки информации: наблюдение, подслушивание, перехват.

Основным проявлением вредоносной или шпионской программы является наличие подозрительного процесса в списке запущенных процессов (программ). Имея достаточную

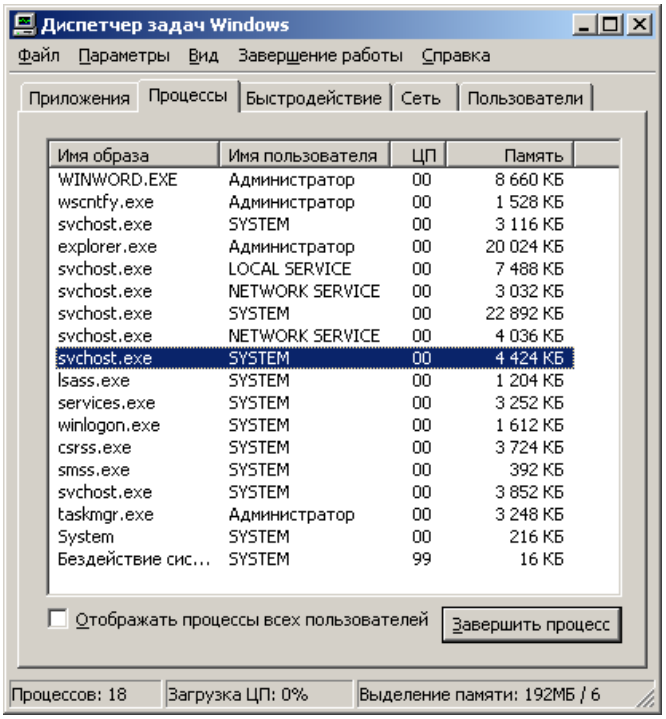
квалификацию можно проанализировать список вручную и выявить вредоносную программу без использования антивирусного ПО. Этот способ является одним из наиболее эффективных для выявления вредоносных программ, имеющих только косвенные или скрытые признаки.

Естественно необходимо четко понимать и уметь отличать легальные процессы (например, системные или запущенные программы) от подозрительных. Для того чтобы посмотреть список запущенных на данный момент программ необходимо воспользоваться **Диспетчером задач Windows**.

Текст задания:

- **Диспетчер задач Windows** - это стандартная утилита, входящая в любую версию Microsoft Windows. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

1. Для того, чтобы открыть **Диспетчер задач Windows** нажмите одновременно клавиши **Ctrl+Alt+Delete.**



Открывшееся окно содержит пять закладок, отвечающих пяти видам активности, которые отслеживает Диспетчер: приложения, процессы, быстродействие (использование системных ресурсов),Сеть и Пользователи. По умолчанию открывается вторая закладка Процессы.

- Если на компьютере не запущены никакие пользовательские программы, список текущих процессов должен содержать только служебные процессы операционной системы.
- **Внимание! Эти процессы необходимы системе для стабильной работы**

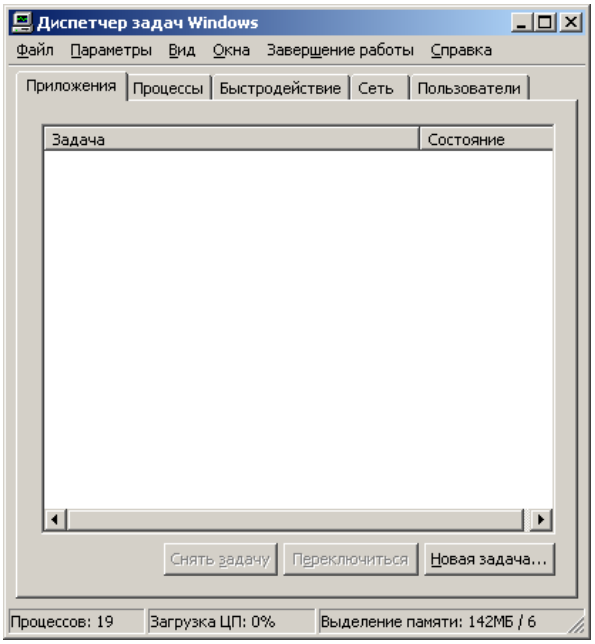
Название	Описание	Возможность

процесса		завершения
CSRSS.EXE	Сокращение от "Client/Server Run – Time Subsystem".Процесс отвечает за окна консоли, за создание и удаление потоков, а также частично за работу 16-битной среды MS-DOS. Он относится к подсистеме Win32 пользовательского режима (WIN32.SYS же относится к ядру Kernel) и должен всегда выполняться.	-
EXPLORER.EXE	Пользовательская среда, содержащая такие компоненты, как Панель задач, Рабочий стол и тому подобное. Его практически всегда можно закрывать и снова открывать без каких-либо последствий.	+
INTERNAT.EXE	Загружает различные выбранные пользователем языки ввода, показывает на панели задач значок "RL", который позволяет переключать языки ввода. С помощью панели управления возможно без использования данного процесса безо всяких проблем переключать раскладку клавиатуры.	+
LSASS.EXE	Этот локальный сервер авторизации отвечает за IP-директивы безопасности (Интернет- протоколы) и загружает драйвер безопасности. Он запускает процесс, отвечающий за авторизацию пользователей. При успешной авторизации пользователя приложение создает и присваивает ему специальный протокол. Все запущенные далее процессы используют этот протокол.	-
MSTASK.EXE	Отвечает за службу планирования Schedule, которая предназначена для запуска различных приложений в определенное пользователем время.	-
SMSS.EXE	Диспетчер сеансов запускает высокоуровневые подсистемы и сервисы. Процесс отвечает за различные действия, например запуск Winlogon- и Win32-процессов, а также за операции с системными переменными. Когда Smss определяем, что Winlogon или Csrss закрыты, он автоматически выключает систему.	-
SPOOLSV.EXE	Обеспечивает создание очереди на печать, временно сохраняя документы и факсы в памяти.	-
SVCHOST.EXE	Этот всеобъемлющий процесс служит хостом для других процессов, запускаемых с помощью DLL. Поэтому иногда работают одновременно несколько Svchost. С помощью команды "tlist - s" можно вывести на экран все процессы, использующие Svchost.	-
SERVICES.EXE	Процесс управления системными службами. Запуск, окончание, а также все остальные действия со службами происходят через него.	-

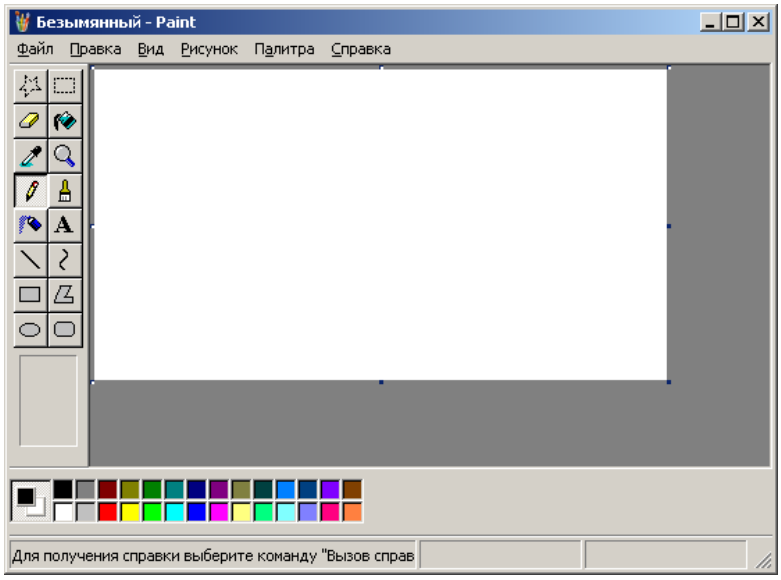
SYSTEM	Этот процесс выполняет все потоки ядра Kernel.	-
SYSTEM IDLE PROCESS	Этот процесс выполняется на любом компьютере. Нужен он, правда, всего лишь для мониторинга процессорных ресурсов, не используемых другими программами.	-
TASKMGR.EXE	Процесс диспетчера задач, закрывать который крайне не рекомендуется.	+
WINLOGON.EXE	Отвечает за управление процессами авторизации пользователей. Он активен, только когда пользователь нажимает "Ctrl+Alt+Del".	-
WINMGTM.EXE	Основной компонент клиентской службы Windows. Процесс запускается одновременно с первыми клиентскими приложениями и выполняется при любом запросе служб. В XP он запускается как клиент процесса Svchost.	-

- Представленные в таблице процессы необходимы для работы Windows XP. В Windows Vista их значительно больше.

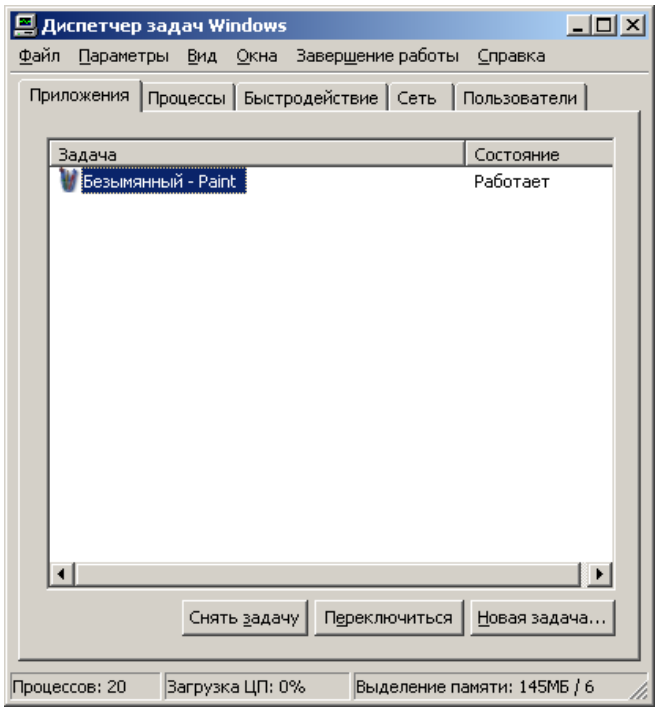
2. Для каждого процесса выводятся его параметры: имя образа, имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти.
3. Поскольку в данный момент не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, "Бездействие системы" должно оказаться внизу списка с достаточно большим процентом "использования" процессора.
4. Если Вы обнаружили подозрительный процесс, не относящийся к системным, завершите его вручную с помощью кнопки "Завершить процесс". Естественно, это не избавляет от наличия вируса на компьютере, а только останавливает его работу в данное время. Далее следует провести проверку с помощью антивируса.
5. Выпишите все запущенные процессы на лист бумаги или в текстовый файл и перейдите к закладке **Приложения**. В данном окне отобразятся все запущенные в настоящий момент приложения. Если в настоящий момент запущенных приложений нет, появится пустое окно, показанное на рис.



6. Не закрывая окна **Диспетчера задач Windows**, откройте программу **Paint**. Для этого воспользуйтесь системным меню **Пуск / Программы / Стандартные / Paint**. Дождитесь запуска **Paint**.

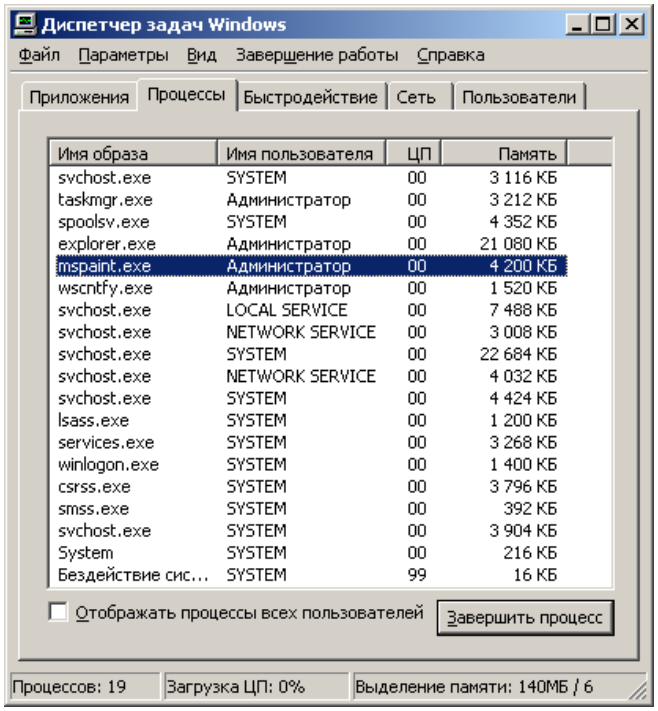


- Не закрывая приложение **Paint**, вернитесь к окну **Диспетчера задач Windows** и проследите за изменениями на закладке **Приложения**. В списке запущенных приложений появился **Paint**.

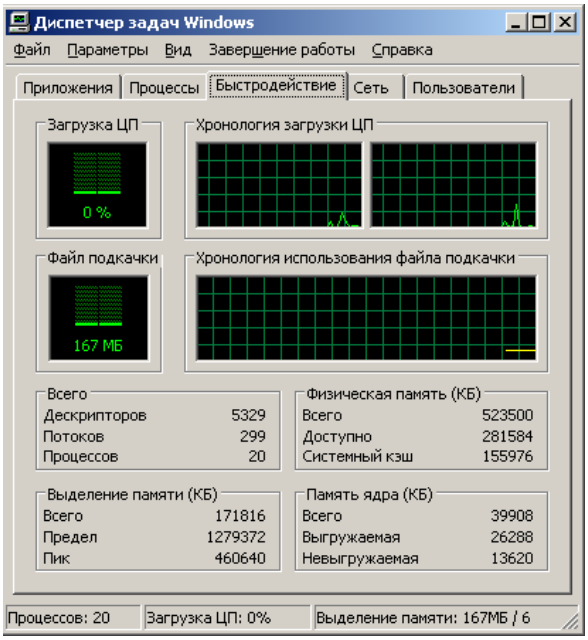


- Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано "Не отвечает". Если некое ранее бесперебойно работающее приложение начало часто без видимых причин переходить в состояние "Не отвечает", это может быть косвенным признаком заражения.

7. Перейдите к закладке **Процессы** и сравните список в тем, который видели ранее. Найдите процесс, соответствующий **Paint**, - **mspaint.exe**.



8. Перейдите к закладке **Быстродействие**. Внимательно изучите расположенные тут графики. Всплески на графиках соответствуют по времени определенным действиям, например, запуску программы, требовательной к ресурсам. Если Вы не запускали ничего, а всплески есть, это может быть причиной для более детального исследования компьютера.



Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительный программы, производящей несанкционированную рассылку писем, связывающейся со своим автором и передающей ему конфиденциальную информацию или просто загружающую свои дополнительные модули или атакующей соседние компьютеры. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть и выдергивать сетевой шнур, увидев необычно яркое мигание лампочки на сетевой карте, необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

Некоторые типы троянских программ специально предназначены для обеспечения удаленного управления зараженным компьютером. Для обеспечения доступа к компьютеру по сети со стороны злоумышленника они открывают определенный порт.

Что такое порт? Как известно, каждый компьютер обладает IP-адресом, на который этому компьютеру можно передавать данные. Но если на компьютере имеется несколько программ, работающих с сетью, например, почтовый сервер и веб-сервер, как определить, какие данные какой программе предназначены? Для этого и используются порты. За каждой программой, ожидающей данные из сети закрепляется определенное число - номер порта, а данные, пересылаемые на компьютер, кроме адреса компьютера содержат также и номер порта, чтобы было понятно, какая программа должна получить эти данные.

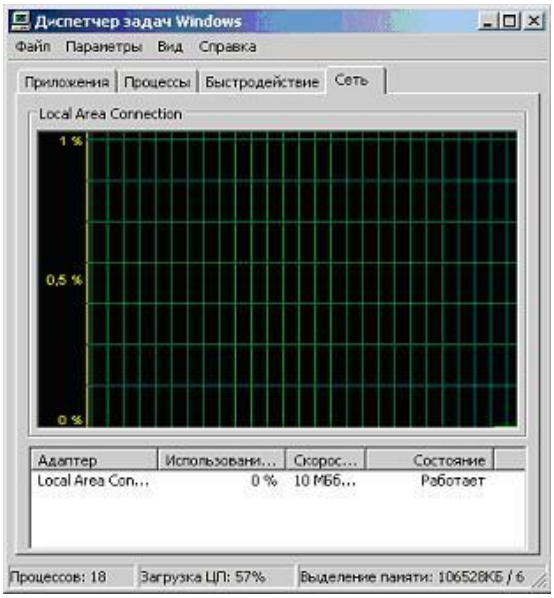
Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно

устанавливаемыми приложениями. В этом задании это предлагается сделать с помощью **Диспетчера задач Windows** и встроенной утилиты netstat, которая выводит на экран мгновенную статистику сетевых соединений.

1. О ткройте окно **Диспетчера задач Windows**, нажав одновременно клавиши **Ctrl, Shift** и **Esc**, и перейдите к закладке **Сеть.**

Поскольку сейчас не инициируется ни одного сетевого соединения, график должен быть пуст, вернее представлять собой прямую на уровне 0 %.

В нижней части окна расположен перечень всех установленных в системе сетевых адаптеров. Обычно он один. В столбце **Использование сети** приводится моментальное значение доли используемого канала, а в **Скорость линии** - пропускная способность. **Состояние** отображает статус.

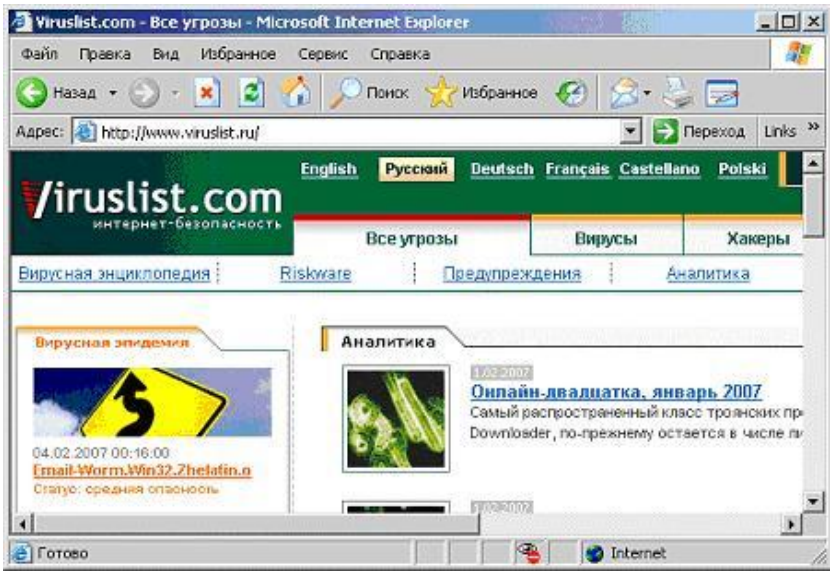


Если на Вашем компьютере нет ни одного активного адаптера, окно **Диспетчера задач** на закладке **Сеть** будет выглядеть так:



В этом задании предполагается, что как минимум один адаптер установлен и работает.

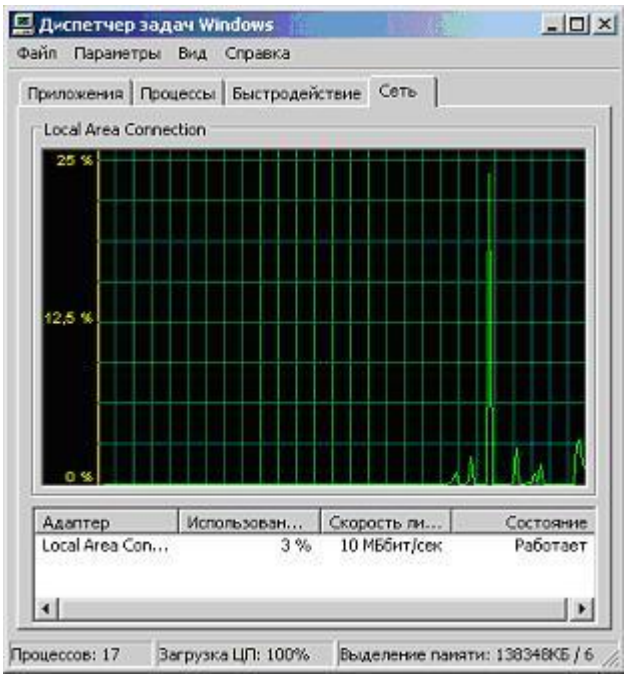
2. Инициируйте какое-нибудь сетевое соединение. Например, откройте браузер и загрузите сайт http://www.securelist.com/ .



При отсутствии выхода в Интернет, зайдите на сетевой ресурс, указанный преподавателем

3. Проследите за изменениями на графике **Диспетчера задач**: все Ваши действия отобразятся на графике в виде пиков сетевой активности, а значение поля **Использование сети** на время перестанет быть равным нулю.

Таким образом, если Вы, закрыв все прикладные программы, которые могут инициировать сетевые соединения, обнаруживаете, что сеть все равно использоваться продолжает, нужно искать причину



Выявление уязвимостей с помощью Microsoft Baseline Security Analyzer

Microsoft Baseline Security analyzer - программа, позволяющая проверить уровень безопасности установленной конфигурации операционной системы (ОС) Windows 2007, XP, Server 2003, Vista, Server 2008. Также проверяется и ряд других приложений разработки Microsoft. Данное средство можно отнести к разряду систем анализа защищенности. Оно распространяется бесплатно и доступно для скачивания с web-сервера Microsoft (адрес http://www.microsoft.com/en-us/download/details.aspx?id=7558).

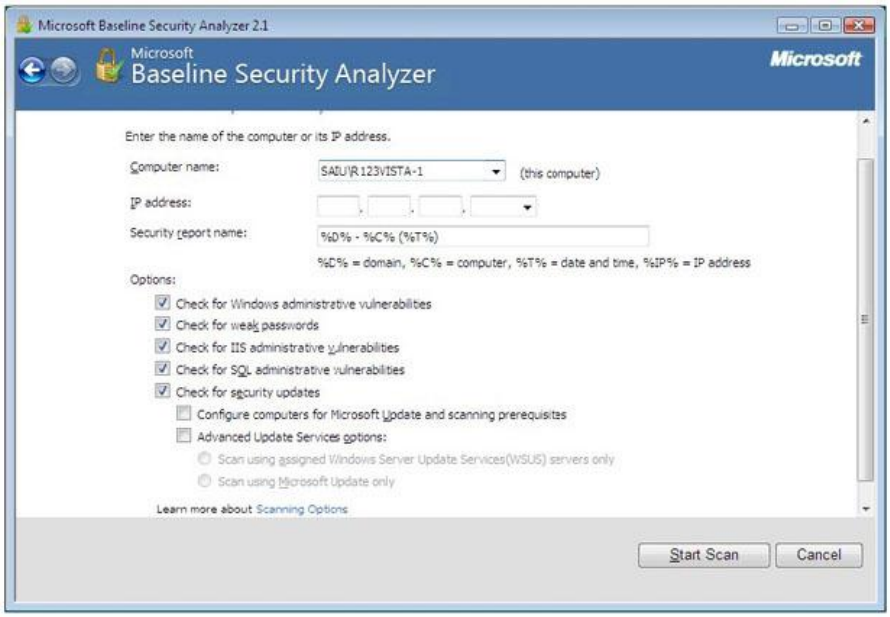
В процессе работы BSA проверяет наличие обновлений безопасности операционной системы, офисного пакета Microsoft Office(для версий XP и более поздних), серверных приложений, таких как MS SQL Server, MS Exchange Server, Internet Information Server и т.д. Кроме того, проверяется ряд настроек, касающихся безопасности, например, действующая политика паролей.

Перейдем к знакомству с программным продуктом. Надо отметить, что при подготовке описания данной лабораторной работы использовалась версия BSA 2.1. К сожалению, продукт не локализован, поэтому использовалась англоязычная версия.

При запуске открывается окно, позволяющее выбрать объект проверки - один компьютер (выбирается по имени или ip-адресу), несколько (задаваемых диапазоном ip-адресов или доменным именем) или просмотреть ранее сделанные отчеты сканирования системы. При выборе сканирования отдельного компьютера по умолчанию подставляется имя локальной станции, но можно указать имя или ip-адрес другого компьютера.



Выбор проверяемого компьютера



Задание параметров проверки

Можно задать перечень проверяемых параметров. На рис. 2 представлен выбор вариантов проверки:

- проверка на наличие уязвимостей Windows, вызванных некорректным администрированием;
- проверка на "слабые" пароли (пустые пароли, отсутствие ограничений на срок действия паролей и т.д.);
- проверка на наличие обновлений безопасности.

Перед началом работы программа обращается на сервер Microsoft для получения перечня обновлений для ОС и известных уязвимостей. Если на момент проведения проверки компьютер не подключен к Интернет, база уязвимостей не будет обновлена, программа об этом сообщит и дальнейшие проверки выполняться не будут. В подобных случаях нужно отключать проверку обновлении безопасности (сбросив соответствующую галочку на экране рис. 2 или с помощью ключа при использовании утилиты командной строки, о чем речь пойдет ниже).

Для успешной проверки локальной системы необходимо, чтобы программа выполнялась от имени учетной записи с правами локального администратора. Иначе проверка не может быть проведена и о чем будет выдано сообщение: "You do not have sufficient permissions to perform this command. Make sure that you are running as the local administrator or have opened the command prompt using the 'Run as administrator' option".

По результатам сканирования формируется отчет, в начале которого дается общая оценка уровня безопасности конфигурации проверяемого компьютера. В приведенном на рис. 3 примере уровень риска оценивается как "серьезный" (Severe risk).

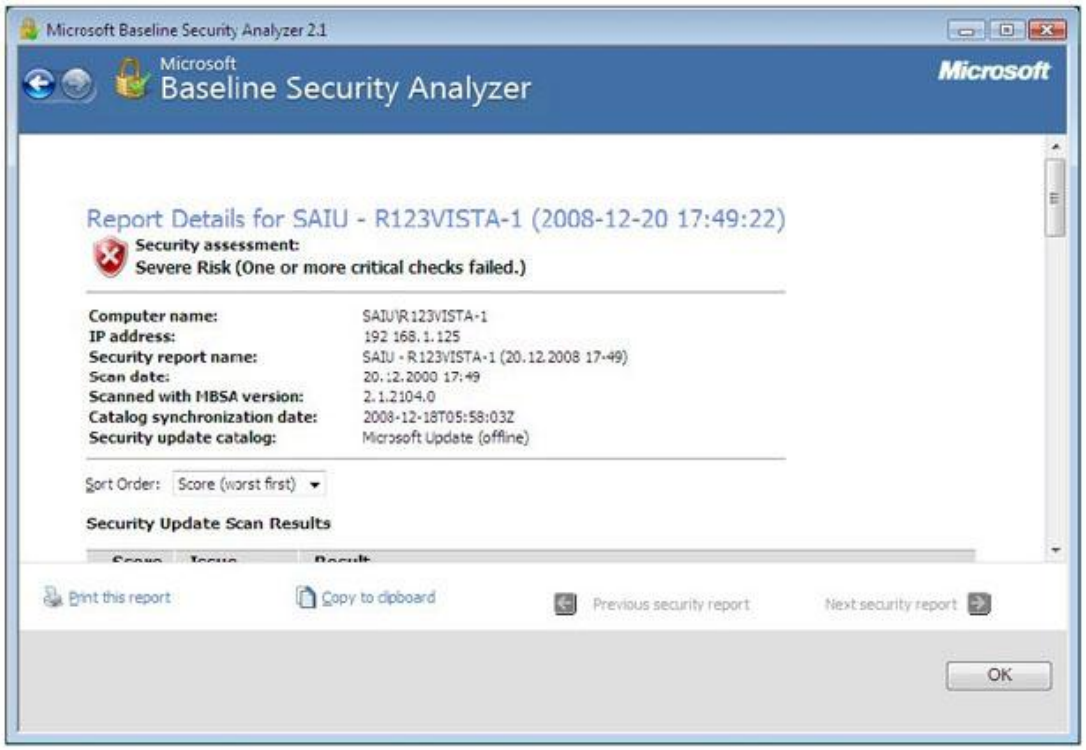


Рис. 3. Заголовок отчета

Далее приводится перечень обнаруженных уязвимостей, разбитый на группы: результаты проверки установки обновлений, результаты проверки Windows и т.д. Надо отметить, что выпускаемые Microsoft обновления бывают различных типов:

Security updates - собственно обновления безопасности, как правило, посвященные исправлению одной уязвимости программного продукта;

Update rollups - набор исправлений безопасности, который позволяет одновременно исправить несколько уязвимостей. Это упрощает обслуживание процесса обновления программного обеспечения (ПО);

Service packs - набор исправлений, как связанных, так и несвязанных с безопасностью. Установка Service pack, как правило, исправляет все уязвимости, обнаруженные с момента выхода предыдущего Service pack, таким образом устанавливать промежуточные обновления уже не надо.

В описании рассматриваемого результата проверки можно выбрать ссылку **Result details** и получить более подробное описание найденных проблем данной группы. При наличии подключения к Интернет, перейдя по приводимой в отчете ссылке, можно получить информацию об отсутствующем обновлении безопасности и скачать его из сети.

Нужно отметить, что установка обновлений для систем с высокими требованиями в области непрерывности работы, требует предварительной тщательной проверки совместимости обновлений с использующимися приложениями. Подобная проверка обычно производится на тестовых системах с близкой конфигурацией ПО. В то же время, для небольших организаций и пользователей домашних компьютеров такая проверка зачастую неосуществима. Поэтому надо быть готовым к тому, чтобы восстановить систему после неудачного обновления. Для современных ОС семейства Windows это можно сделать, например, используя специальные режимы загрузки ОС - безопасный режим или режим загрузки последней удачной конфигурации.

Также надо отметить еще одну особенность. На данный момент **baseline security analyzer** не существует в локализованной русскоязычной версии. И содержащиеся там ссылки на пакеты обновлений могут указывать на иные языковые версии, что может создать проблемы при обновлении локализованных продуктов.



Перечень неустановленных обновлений (по группам)



Уязвимости, связанные с администрированием операционной системы

налогичным образом проводится работа по анализу других групп уязвимостей (рис. 5). Описывается уязвимость, указывается ее уровень критичности, даются рекомендации по исправлению. На рис. 6 представлено подробное описание результатов (ссылка **result details**) проверки паролей. Указывается, что 3 учетные записи имеют пароли, неограниченные по сроку действия.



Результаты проверки паролей

<u>Дополнительные задания</u>

1. Выполните проверку Вашего компьютера с помощью Microsoft Baseline security analyzer. В отчете о выполнении практической работы укажите:

- как оценен уровень уязвимости Вашего компьютера;
- какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;

HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке \%System-root%\System32\Confiq
HKEY_LOCAL_MACHINE\SECURITY	Содержит информацию безопасности в файлах SECURITY.SECURITY.LOG, SECURITY.SAV в папке \%Systemroot%\System32\Confiq
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлахSYSTEM.SYSTEM.LOG, SYSTEM.SAV в папке \%Systemroot%\System32\Config
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этой ветви, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке \%Systemroot%\System32\Config
HKEY_USERS\DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке \%Systemroot%\System32\Confiq
HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и - NTUSER.DAT.LOG, расположенных в каталоге \%Systemroot%\Profiles\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент

- опишите наиболее серьезные уязвимости каждого типа, выявленные на Вашем компьютере
- Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.

Работа с реестром в Windows

Реестр операционной системы Windows - это иерархически построенная база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра.

Реестр формируется из различных данных. Чтобы получилось то, что видит пользователь, редактируя реестр, происходит следующее.

Вначале, в процессе установки и настройки Windows, на диске формируются файлы, в которых хранится часть данных относительно конфигурации системы.

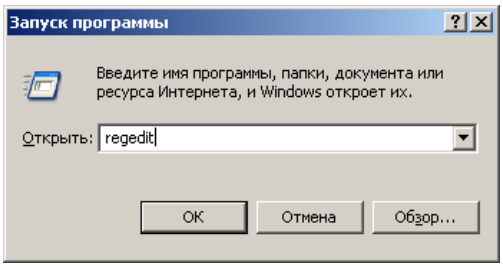
Затем, в процессе каждой загрузки системы, а также в процессе каждого входа и выхода каждого из пользователей, формируется некая виртуальная сущность, называемая "реестром" — объект REGISTRY\. Данные для формирования "реестра" частично берутся из тех самых файлов (Software, System …), частично из информации, собранной ntdetect при загрузке (HKLM\Hardware\Description).

То есть часть данных реестра хранится в файлах, а часть данных формируется в процессе загрузки Windows.

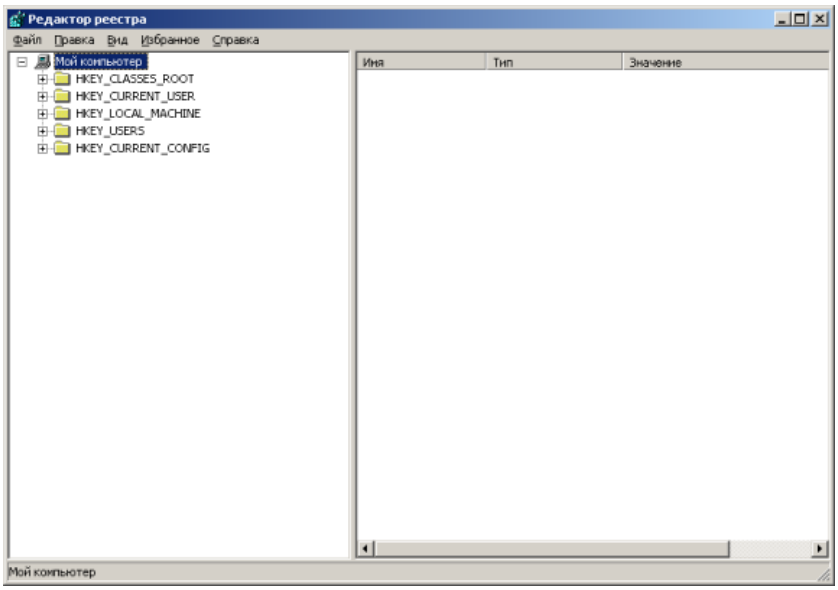
Характеристики основных разделов реестра представлены в таблице.

Основным средством для просмотра и редактирования записей реестра служит специализированная утилита **"Редактор реестра"**.

Для того чтобы открыть редактор реестра откройте Пуск->Выполнить. В окне введите **regedit**.



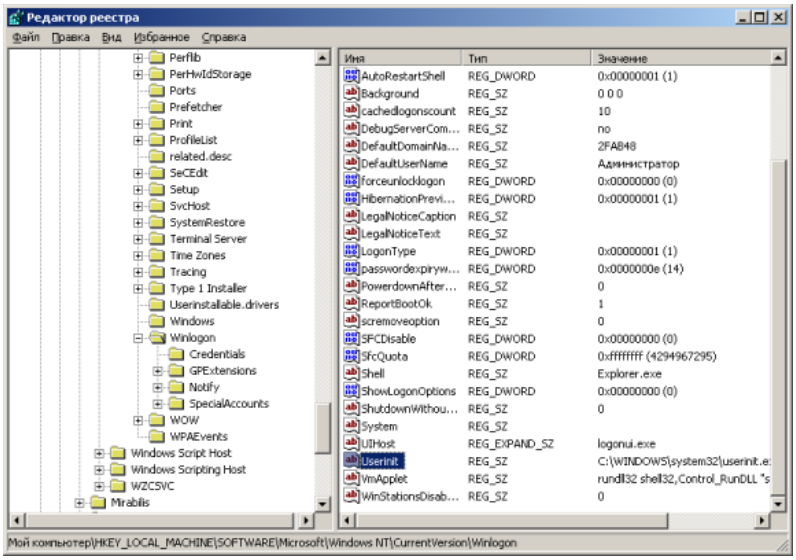
Откроется окно редактора реестра.



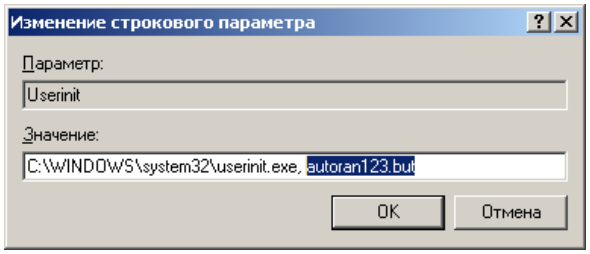
В левой части окна находится дерево ключей реестра, ключи изображены в виде папок. В правой части окна отображаются записи, относящиеся к выбранному ключу. В ключе могут находиться и записи — параметры настройки, и другие ключи — группы параметров настройки.

Вредоносные программы, как и любые программы, для работы нуждаются в запуске. Поэтом они часто используют реестр, в частности, его разделы, отвечающие за автоматический запуск программ при загрузке операционной системы.

1. Откройте Редактор реестра.
2. В ветви **HKEY_LOCAL_MACHINE** выберите **Software\Microsoft\WindowsNT\CurrentVersion\Winlogon.**
3. В правой половине окна появится список ключей для данной ветви. Найдите ключ **Userinit** и проверьте его содержимое.



Нормальным значением данного ключа является запись **C:\WINDOWS\system32\userinit.exe** . Наличие в ключе других записей может свидетельствовать о наличии на компьютере вредоносных программ. Для удаления из ключа подозрительной записи щелкните на нем два раза левой кнопкой мыши. После редактирования нажмите ОК.



Далее перейдите в папку, где находится подозрительный файл и удалите его вручную. После этого перезагрузите систему. Если после перезагрузки в ключе удаленное значение не появилось снова – система вылечена.

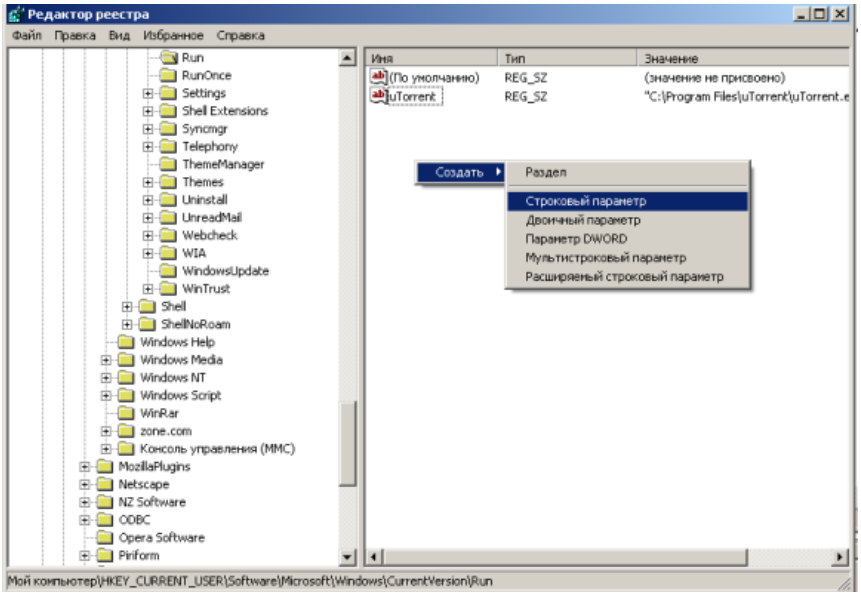
Как уже говорилось выше, любимым местом вредоносных программ являются разделы реестра, отвечающие за автозапуск.

В реестре автозагрузка представлена в нескольких местах:

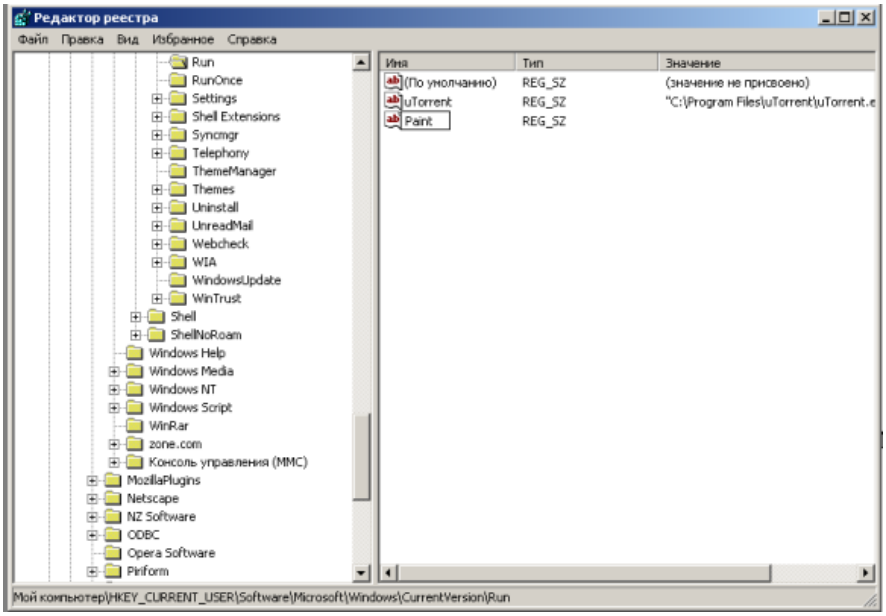
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run** - программы, которые запускаются при входе в систему. Данный раздел отвечает за запуск программ для всех пользователей системы.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce** - программы, которые запускаются только один раз при входе пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx** - программы, которые запускаются только один раз, когда загружается система. Этот раздел используется при инсталляции программ, например для запуска настроечных модулей. После этого ключи программ автоматически удаляются из данного раздела реестра. Данный раздел отвечает за запуск программ для всех пользователей системы.
- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run** - программы, которые запускаются при входе текущего пользователя в систему
- **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce** - программы, которые запускаются только один раз при входе текущего пользователя в систему. После этого ключи программ автоматически удаляются из данного раздела реестра.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices** - программы, которые загружаются при старте системы до входа пользователя в Windows.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce** - программы отсюда загружаются только один раз, когда загружается система.

1. Откройте Редактор реестра

2. Откройте следующий раздел HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
3. В правой части окна вызовите правой кнопкой мыши контекстное меню и выберите ***Создать->Строковый параметр***



4. Задайте имя для создаваемого параметра.



5. Откройте вновь созданный параметр и задайте ему значение в виде пути к исполняемому файлу Paint - **C:\WINDOWS\System32\mspaint.exe**
6. Нажмите ОК и перезагрузите компьютер. Paint загрузится автоматически после загрузки операционной системы.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если все шаги выполнены полностью правильно и самостоятельно, а аспирант способен уверенно отвечать на вопросы преподавателя о проделанной работе;

Оценка «хорошо» выставляется, если работа выполнена в целом корректна, но имеются неточности в ответах на вопросе преподавателя или некоторые действия выполнены неоптимально;

Оценка «удовлетворительно» выставляется, когда работа не может быть завершена аспирантом самостоятельно, без помощи преподавателя.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 6. Принципы добывания и обработки информации техническими средствами

Тематика: Способы и средства наблюдения в радиодиапазоне.

Цель: проанализировать средства радио- и радиотехнической разведки, их принципы работы, назначение, параметры и особенности применения, техническое исполнение.

Текст задания: Проанализируйте средства радио- и радиотехнической разведки. Составьте обзор рынка современных средств радио- и радиотехнической разведки. Оформите отчет в виде текстового файла и презентации к сообщению (будьте готовы к выступлению с этим отчетом).

Методические рекомендации:

При анализе средств радио- и радиотехнической разведки обратите внимание на отражение следующих вопросов:

- назначение;
- возможности;
- принципы работы средств ТР;
- характеристики;
- преимущества и недостатки;
- техническая реализация.

Средства радио- и радиотехнической разведки для анализа:

1. Сканирующие радиоприемники.
2. Радиопеленгаторы.
3. Анализаторы электромагнитного поля.
4. Аппаратура поиска несанкционированных излучений.
5. Частотомеры.
6. Анализаторы спектра.

Контрольные вопросы:

По каждому виду средств радио- и радиотехнической разведки опишите:

- назначение средства;
- принципы работы средств;
- преимущества и недостатки;
- наиболее распространенная техническая реализация.

Рекомендуется использовать источник: Бюро Научно-Технической Информации «Каталог технических средств для спецслужб». URL: http://www.bnti.ru/.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если при анализе средств технической разведки на все вопросы дан развернутый и правильный ответ.

Оценка «хорошо» за практическую работу выставляется, если при анализе средств технической разведки были учтены не все вопросы, требующие освещения согласно методическим рекомендациям.

Оценка «удовлетворительно» за практическую работу выставляется, если аспирант собрал всю необходимую информацию о средствах технической разведки, но затрудняется при составлении их сравнительного анализа.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 7. Классификация и структура технических каналов утечки информации

Тематика: Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.

Цель: проанализировать средства акустической разведки, их принципы работы, параметры и особенности применения.

Текст задания: Проанализируйте средства акустической разведки. Составьте обзор рынка современных средств акустической разведки. Оформите отчет в виде текстового файла и презентации к сообщению (будьте готовы к выступлению с этим отчетом).

Методические рекомендации:

При анализе средства акустической разведки обратите внимание на отражение следующих вопросов: назначение средства, принципы работы средств АР, параметры, влияющие на дальность работы, характеристики, преимущества и недостатки, техническая реализация, способы внедрения средств АР.

Средства радио- и радиотехнической разведки для анализа:

1. Телефонные закладки.
2. Проводные микрофоны.
3. Направленные параболические микрофоны.
4. Лазерные микрофоны.
5. Портативные диктофоны и транскрайберы.
6. Электронные стетоскопы
7. Закладные устройства.
8. «Телефонное ухо»

Контрольные вопросы:

По каждому виду средств акустической разведки опишите:

- назначение средства;
- принципы работы средств АР;
- преимущества и недостатки;
- наиболее распространенная техническая реализация.

Рекомендуется использовать источник: Бюро Научно-Технической Информации «Каталог технических средств для спецслужб». URL: http://www.bnti.ru/.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если при анализе средств технической разведки на все вопросы дан развернутый и правильный ответ.

Оценка «хорошо» за практическую работу выставляется, если при анализе средств технической разведки были учтены не все вопросы, требующие освещения согласно методическим рекомендациям.

Оценка «удовлетворительно» за практическую работу выставляется, если аспирант собрал всю необходимую информацию о средствах технической разведки, но затрудняется при составлении их сравнительного анализа.

Оценка «неудовлетворительно» выставляется, если работа не была выполнена.

Практическое занятие 8. Средства предотвращения утечки информации по техническим каналам

Тематика: Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств.

Текст задания: Найдите ответы на предложенные ниже вопросы, используя возможности поисковых систем.

1. Перечислите методы защиты акустической информации. Раскройте их содержание.
2. Сформулируйте цель применения пассивных средств защиты информации.
3. Сформулируйте цель применения звукоизоляции.
4. Назовите способы уменьшения утечки акустической информации через окна и двери.
5. Назовите характеристики звукопоглощающих свойств различных конструкций.
6. Охарактеризуйте виды звукопоглощающих материалов.
7. Перечислите активные способы защиты акустической информации.
8. Охарактеризуйте виды помех, используемые для зашумления.
9. Разъясните суть создания акустических помех с указанием принципа защиты каждого средства и конкретными примерами устройств.
10. Перечислите рекомендации к защищаемым помещениям, размещаемым в пределах контролируемой зоны (КЗ) (в соответствии с СТР-К).
11. Что такое система охранного телевидения? Цель ее создания?
12. Перечислите виды видеокамер и их параметры.

Шкала оценивания:

Оценка «отлично» за практическую работу выставляется, если на все вопросы дан полный, обоснованный и правильный ответ;

Оценка «хорошо» выставляется, если аспирант ошибся при ответе на один-два вопроса;

Оценка «удовлетворительно» выставляется, если аспирант ошибся при ответе на три-четыре вопроса.

Оценка «неудовлетворительно» выставляется, если аспирант допустил больше четырех ошибок.

Практическое занятие 9. Заключительное занятие. Подведение и анализ промежуточных результатов освоения дисциплины

При подготовке материалов для заключительного практического занятия, преподаватель учитывает недостаточную степень развития навыков аспирантов, определенную в ходе практических занятий и при оценке самостоятельной работы. На практическом занятии обсуждаются итоги проведения занятий по дисциплине, проверяется полнота и качество собранного аспирантом портфолио материалов и результатов выполнения заданий по дисциплине. Обсуждаются вопросы, вынесенные для проведения зачета с оценкой, итоги

выполнения работы по написанию рефератов. Оцениваются индивидуальные достижения, полученные аспирантов в ходе внеурочной работы (сертификаты олимпиад, конкурсов, грантов, написание тезисов/статей в сборники конференций различного уровня).

3. Методические указания по выполнению других видов самостоятельной работы по дисциплине

ТЕМЫ РЕФЕРАТОВ

1. Нормативно-правовые документы технической ЗИ
2. Структура контролирующих органов по ЗИ
3. История развития технической разведки
4. «Детекторы лжи» и их использование для получения информации
5. Средства и методы (не меньше двух) обнаружения закладных устройств
6. Средства для проведения скрытой фотосъемки
7. Защита от визуально-оптических и фотографических средств разведки
8. Способы пассивного скрытия (маскировка)
9. Перехват телефонных переговоров в зонах «А», «Б», «В»
10. Приборы ночного видения и тепловизоры
11. Радиоприёмники и их характеристики
12. Способы и средства прослушивания, слуховая система человека
13. Направленные и лазерные микрофоны
14. Мобильные системы связи и их использование в информационных атаках
15. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него

Критерии оценки

Оценки в баллах	Критерии
2	Самостоятельность в подготовке материала
3	Аргументированность и полнота материала
2	Использование современной и актуальной литературы
3	Качество презентации
10	**Итого**

Шкала оценивания:

– оценка «отлично» выставляется аспиранту, если сумма баллов по всем критериям равна 9-10 баллам;

– оценка «хорошо» выставляется аспиранту, если сумма баллов по всем критериям равна 7-8 баллам;

– оценка «удовлетворительно» выставляется аспиранту, если сумма баллов по всем

критериям равна 5-6 баллам;

– оценка «неудовлетворительно» выставляется аспиранту, если сумма баллов по всем критериям равна 1-4 баллам.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ЗАЧЕТА С ОЦЕНКОЙ

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
2. Принципы защиты информации техническими средствами.
3. Основные направления инженерно-технической защиты информации.
4. Показатели эффективности инженерно-технической защиты информации.
5. Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.
6. Семантическая информация, циркулирующая в человеческом обществе. Профессиональные языки.
7. Признаковая информация. Информация о видовых признаках, о признаках сигналов, о признаках веществ.
8. Структурирование информации.
9. Классификация демаскирующих признаков.
10. Опознавательные признаки и признаки деятельности.
11. Видовые демаскирующие признаки.
12. Демаскирующие признаки сигналов.
13. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.
14. Виды источников и носителей информации.
15. Прямые и косвенные источники семантической информации.
16. Принципы записи и съема информации с её носителя.
17. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции.
18. Побочные электромагнитные излучения и наводки
19. Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.
20. Технические каналы утечки информации: наблюдение, подслушивание, перехват.
21. Источники угроз безопасности информации.
22. Опасные сигналы и их источники.
23. Способы и средства наблюдения в оптическом диапазоне. Обработка информации в оптическом приемнике.
24. Способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов.
25. Обработка информации в радиоприемнике.
26. Способы и средства подслушивания. Обработка информации в акустическом приемнике.
27. Типовая структура и виды технических каналов утечки информации.
28. Каналы утечки речевой информации.
29. Каналы утечки информации при её передаче по каналам связи.

30. Каналы утечки видовой информации.

31. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.

32. Каналы утечки информации за счет побочных электромагнитных излучений и наводок.

33. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.

34. Средства звукоизоляции из звукопоглощения.

35. Средства обнаружения, локализации и подавления сигналов закладных устройств.

36. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.

37. Генераторы линейного и пространственного зашумления.

По представленным вопросам предполагается выполнение аспирантом конспектов или повторение материала с использованием конспектов лекций.

4. Примеры контрольных заданий (оценочных средств), используемых при текущем контроле успеваемости и промежуточной аттестации по дисциплине

Демоверсия итогового тестирования:

1. Как называются методы защиты акустической информации, направленные на ослабление непосредственных акустических сигналов, циркулирующих в помещении?

а) активные;

б) пассивные (правильный ответ);

в) проактивные;

г) превентивные.

2. Как называются методы защиты акустической информации, предусматривающие создание маскирующих помех?

а) активные (правильный ответ);

б) пассивные;

в) проактивные;

г) превентивные.

3. Звукопоглощение основано на:

а) превращении кинетической энергии в потенциальную (правильный ответ);

б) превращении потенциальной энергии в кинетическую;

в) превращении потенциальной энергии в свободную;

г) превращении кинетической энергии в свободную.

4. Какое средство чаще всего используется злоумышленником для снятия информации в виброакустическом канале утечки?

а) микрофон;

б) лазер;

в) стетоскоп (правильный ответ);

г) анализатор спектра.

5. Что использует “телефонное ухо” для передачи информации злоумышленнику?

а) телефонную линию (правильный ответ);

б) силовую линию;

в) радиоканал;

г) оптический канал.

6. К какому типу методов защиты информации от утечки через ПЭМИН относится экранирование?

а) пассивные (правильный ответ);

б) ручные;

в) организационные;

г) активные.

7. На какой срок выдается лицензия на техническую защиту конфиденциальной информации?

а) 1 год;

б) 3 года;

в) 5 лет;

г) бессрочная (правильный ответ).

8. Что необходимо получить для официального подтверждения эффективности используемых мер и средств по защите информации на объекте информатизации?

а) лицензию;

б) аттестат (правильный ответ);

в) решение;

г) сертификат.

Автор(ы)-составитель(и): *Привалов А.Н.*, профессор кафедры математики, информатики и методики обучения, доктор технических наук, профессор