МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал ордена Трудового Красного Знамени
федерального государственного бюджетного образовательного учреждения
высшего образования
«Московский технический университет связи и информатики»

А.Г. ЖУКОВСКИЙ

Методические указания
По выполнению практического занятия №2
по дисциплине

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К ИСТОЧНИКАМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Направление подготовки 09.03.01 Информатика и вычислительная техника

Ростов-на-Дону
2022

Методические указания
по выполнению практического занятия №2
по дисциплине
«Основы информационной безопасности»

Составитель: А.Г. Жуковский, проф. каф. «ИТСС»

Рассмотрено и одобрено
на заседании кафедры «ИТСС»
Протокол от «19» декабря 2022 г., №5.

Практическое занятие №2.

ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

1.1.Общие положения

Защита информации от утечки по техническим каналам — это комплекс организационных, организационно -технических и технических мероприятий, исключающих или ослабляющих бесконтрольный выход конфиденциальной информации за пределы контролируемой зоны.

К факторам вызывающим утечку информации могут относиться:

- недостаточное знание работниками предприятия правил защиты информации и непонимание (или недопонимание) необходимости их тщательного соблюдения;

- использование неаттестованных технических средств обработки конфиденциальной информации;

- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;

- текучесть кадров, в том числе владеющих сведениями конфиденциального характера.

Таким образом, большая часть причин и условий, создающих предпосылки и возможность утечки конфиденциальной информации, возникает из-за недоработок руководителей предприятий и их сотрудников.

Кроме того, утечке информации способствуют:

- стихийные бедствия (шторм, ураган, смерч, землетрясение, наводнение);

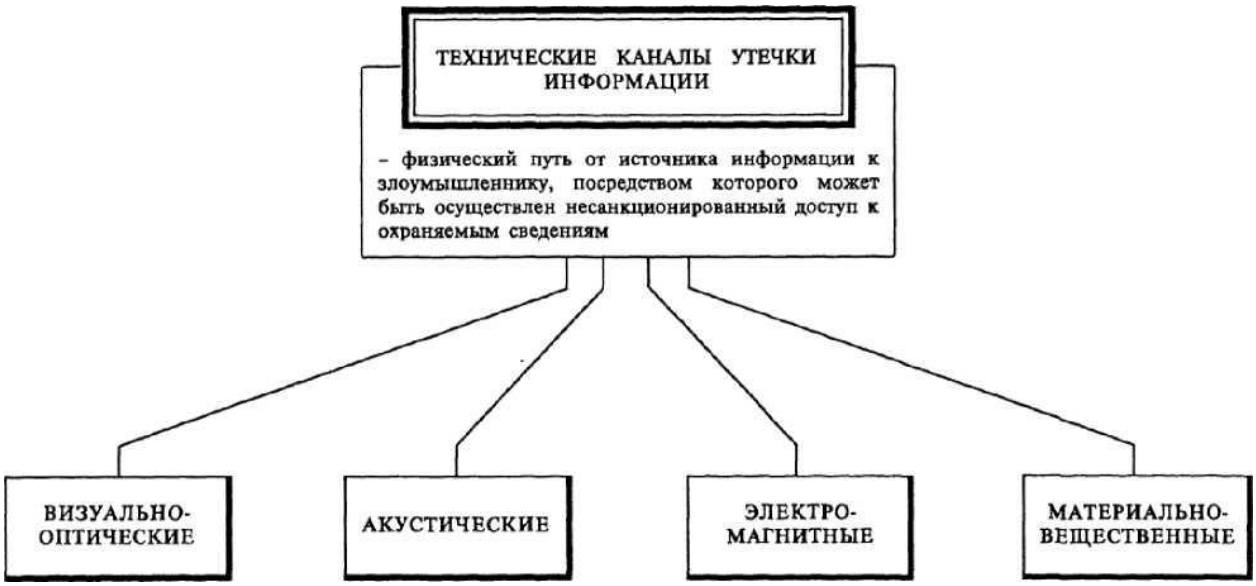
- неблагоприятная внешняя среда (гроза, дождь, снег);

- катастрофы (пожар, взрывы);

- неисправности, отказы, аварии технических средств и оборудования.

По физической природе возможны следующие средства переноса информации:

- световые лучи;
- звуковые волны;
- электромагнитные волны;
- материалы и вещества.

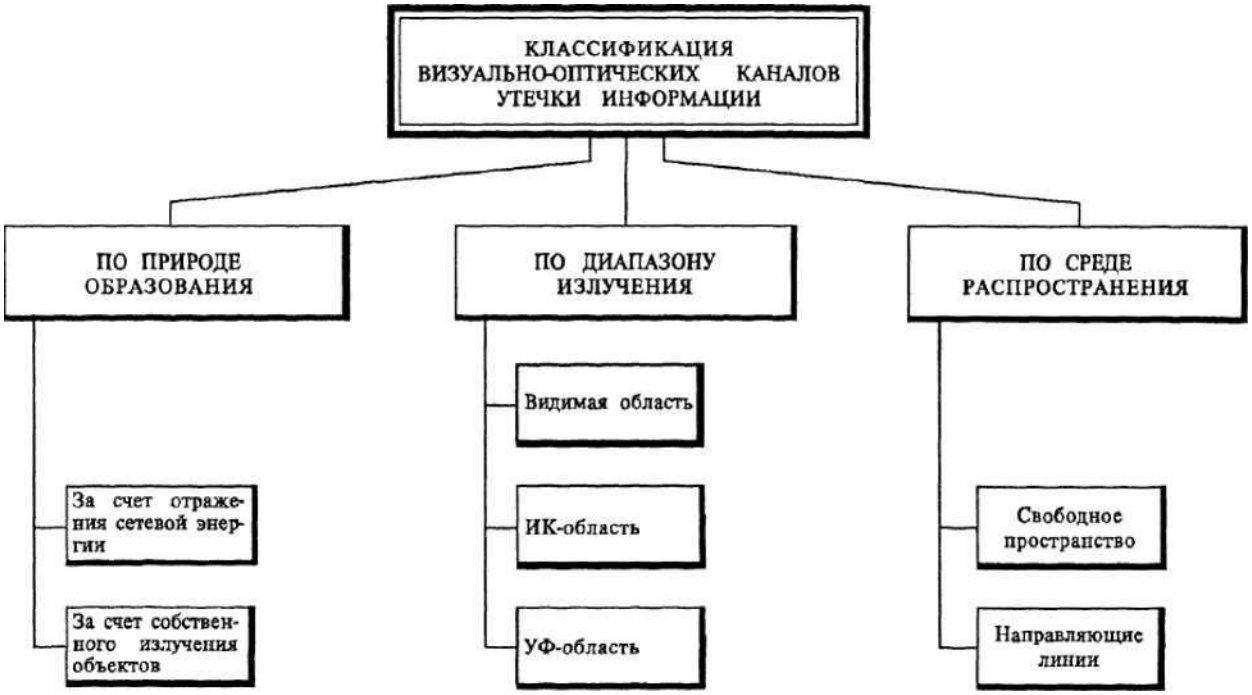


Движение информации в таком канале осуществляется только в одну сторону — от источника к злоумышленнику.

СТРУКТУРА КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

1.2.Защита информации от утечки по визуально оптическим каналам

Визуально-оптические каналы — это, как правило, непосредственное или удаленное (в том числе и телевизионное) наблюдение. Переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах



Поэтому одним из довольно распространенных каналов утечки информации является акустический канал. В акустическом канале переносчиком информации выступает звук, лежащий в полосе ультра (более 20 000 Гц), слышимого и инфразвукового диапазонов. Диапазон звуковых частот, слышимых человеком, лежит в пределах от 16 до 20 000 Гц, и содержащихся в человеческой речи — от 100 до 6000 Гц.

Защита информации от утечки по визуально -оптическому каналу — это комплекс мероприятий, исключающих или уменьшающих

возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии.

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

- располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника (пространственные ограждения);

- уменьшить отражательные свойства объекта защиты;

- уменьшить освещенность объекта защиты (энергетические ограничения);

- использовать средства преграждения или значительного ослабления отраженного света: ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;

- применять средства маскирования, имитации и другие с целью защиты и введения в заблуждение злоумышленника;

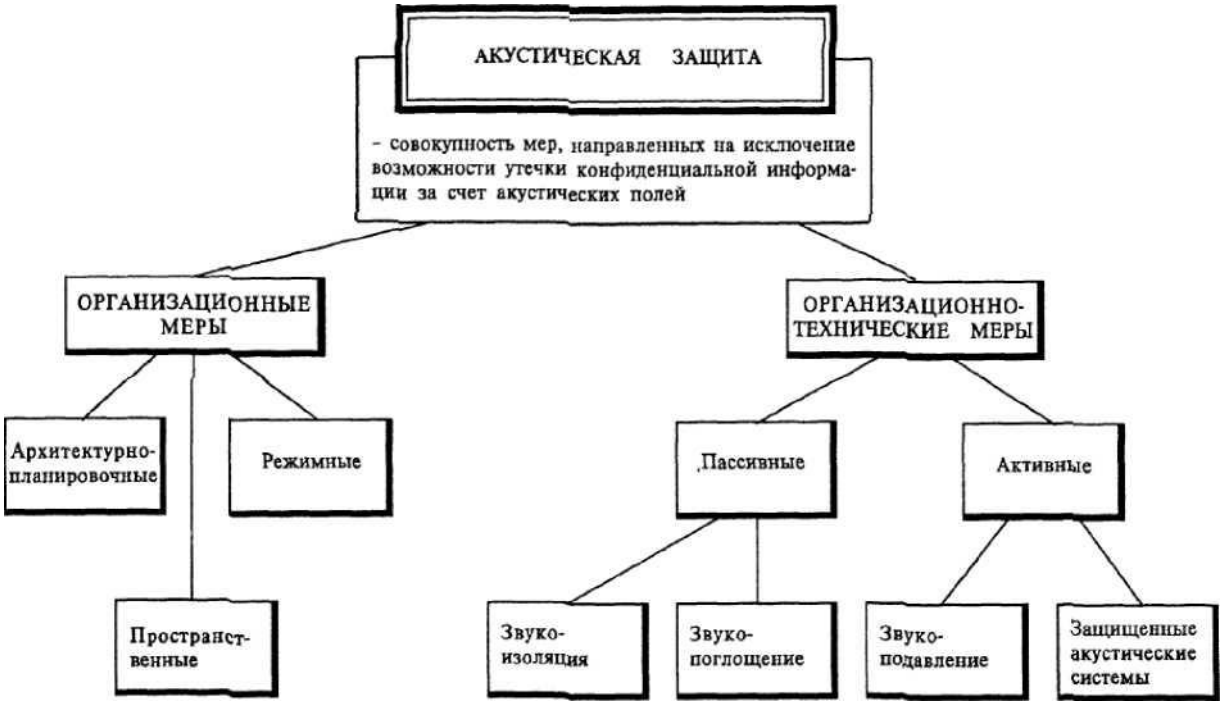
- использовать средства пассивной и активной защиты источника от неконтролируемого распространения отражательного или излученного света и других излучений;

- осуществлять маскировку объектов защиты, варьируя отражательными свойствами и контрастом фона;

- применять маскирующие средства сокрытия объектов можно в виде аэрозольных завес и маскирующих сеток, красок, укрытий.

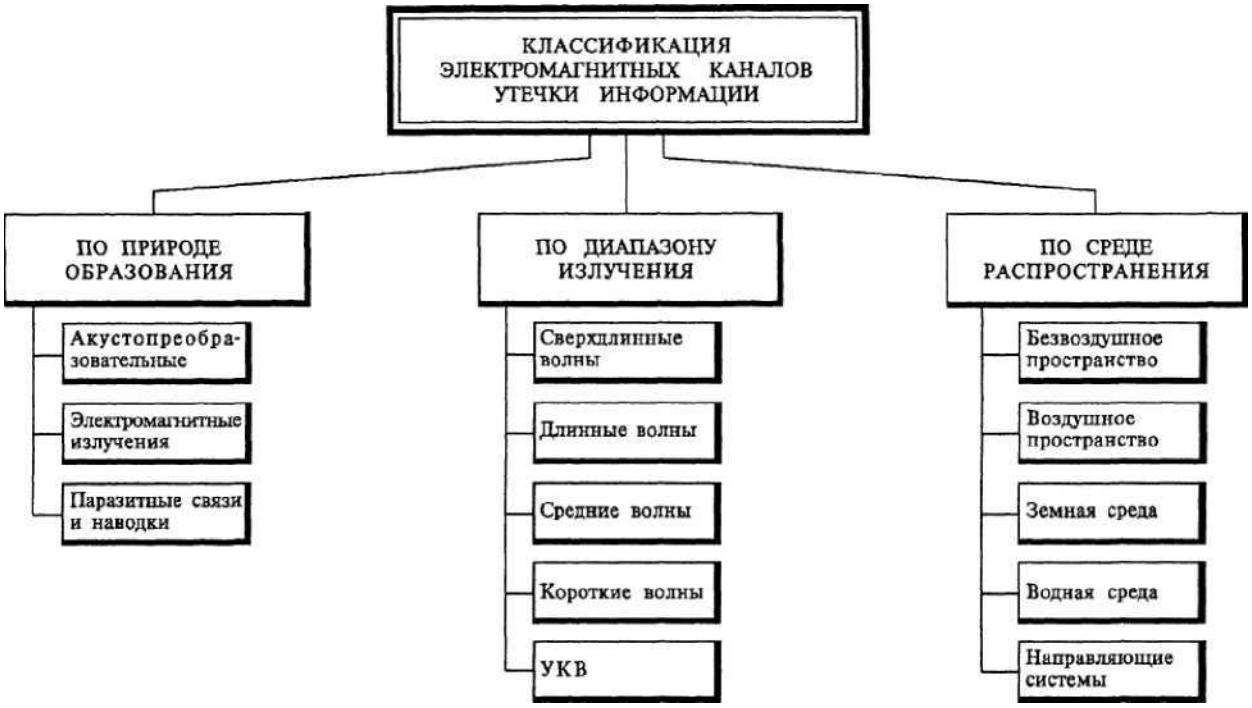
1.3.Защита информации от утечки по акустическим каналам

Защита информации от утечки по акустическому каналу — это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей.



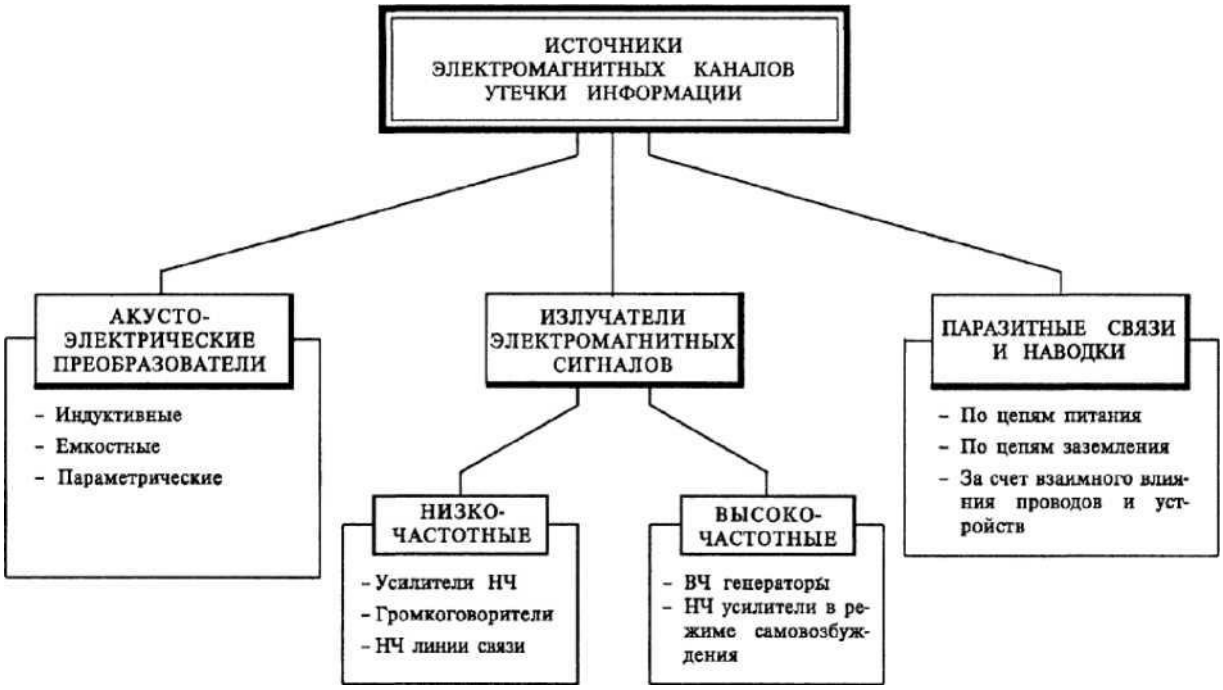
1.4.Защита информации от утечки по электромагнитным каналам

Электромагнитные каналы. Переносчиком информации являются электромагнитные волны в диапазоне от сверхдлинных с длиной волны 10 000 м (частоты менее 30 Гц) до субмиллиметровых с длиной волны 1—0,1 мм (частоты от 300 до 3000 ГГц). Каждый из этих видов электромагнитных волн обладает специфическими особенностями распространения как по дальности, так и в пространстве.



Известны следующие электромагнитные каналы утечки информации:

- микрофонный эффект элементов электронных схем;
- электромагнитное излучение низкой и высокой частоты;
- возникновение паразитной генерации усилителей различного назначения;
- цепи питания и цепи заземления электронных схем;
- взаимное влияние проводов и линий связи;
- высокочастотное навязывание;
- волоконно -оптические системы.



Побочные электромагнитные излучения и наводки (ПЭМИН) присущи любым электронным устройствам, системам, изделиям по самой природе проявления.

Защита от утечки информации за счет побочных электромагнитных излучений самого различного характера предполагает:

- размещение источников и средств на максимально возможном удалении от границы охраняемой (контролируемой) зоны;

- экранирование зданий, помещений, средств кабельных коммуникаций;

- использование локальных систем, не имеющих выхода за пределы охраняемой территории (в том числе систем вторичной часофикации, радиофикации, телефонных систем внутреннего пользования, диспетчерских систем, систем энергоснабжения и т. д.);

- развязку по цепям питания и заземления, размещенных в границах охраняемой зоны;

- использование подавляющих фильтров в информационных цепях, цепях питания и заземления.

Для обнаружения и измерения основных характеристик ПЭМИ используются:

- измерительные приемники;

- селективные вольтметры;

- анализаторы спектра;

- измерители мощности и другие специальные устройства.

1.5 Защита информации от утечки по материально - вещественным каналам

Материально-вещественными каналами утечки информации выступают самые различные материалы в твердом, жидком и газообразном или корпускулярном (радиоактивные элементы) виде. Очень часто это различные отходы производства, бракованные изделия, черновые материалы и другое.

Защита информации от утечки по материально – вещественному каналу — это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов.

При защите информации от утечки по любому из рассмотренных каналов следует придерживаться следующего порядка действий:

1. Выявление возможных каналов утечки.
2. Обнаружение реальных каналов.
3. Оценка опасности реальных каналов.
4. Локализация опасных каналов утечки информации.
5. Систематический контроль за наличием каналов и качеством их защиты.

2. Содержание отчета

1. По указанию преподавателя студенту или группе студентов предлагается выработать комплекс защитных мероприятий от утечки

информации для определенного типа предприятия или организации (определяется также преподавателем).

2. В отчете должны быть изложены конкретные меры защиты с учетом рассмотренных выше технических мероприятий.

3. Выводы по проведенной работе, в которых указаны особенности применяемых мер защиты.

3. Список использованных источников

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат)

2. Е. Б. Белов, В. Лось, Р. В. Мещеряков, Д. А. Шелупанов. Основы информационной безопасности. М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60x88 1/16. - (Специальность; Учебное пособие для высших учебных заведений.

3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам М.:Гор. линия-Телеком, 2015. - 586 с.: 60x90 1/16 (Обложка) ISBN 978-5-9912-0424-8

4. Ярочкин В.И. Информационная безопасность .М.: Академический Проект, 2008. — 544 с. — 978-5-8291-0987-5. — Режим доступа:

5. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации СПб. : Университет ИТМО, 2011. — 112 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/65808.html

6. Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. — М.: Гелиос АРВ, 2005. —192 с.

7. Основы информационной безопасности: курс лекций: учебное пособие / Издание третье / Галатенко В. А. Под редакцией академика РАН В. Б. Бетелина / — М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. — 208 с.