Лабораторный практикум.
СОДЕРЖАТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ РУКОВОДЯЩИХ, НОРМАТИВНЫХ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ПРОТИВОДЕЙСТВИЮ ТЕХНИЧЕСКОЙ РАЗВЕДКЕ.

Володин Сергей Михайлович
К.т.н., доцент кафедры
Информационные системы и технологии

Анализ руководящих и нормативно-методические документов, регламентирующих деятельности в области защиты информации

К руководящим документам в области защиты информации относятся: "Доктрина информационной безопасности Российской Федерации", утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895; Федеральный закон от 27.07.2006 г. № 149-ФЗ "Об информации, информационных технологиях и защите информации"; Федеральный закон от 04.07.96 г. № 85-ФЗ "Об участии в международном информационном обмене"; Федеральный закон от 16.02.95 г. № 15-ФЗ "О связи"; Федеральный закон от 26.11.98 г. № 178-ФЗ "О лицензировании отдельных видов деятельности"; Указ Президента Российской Федерации от 19.02.99 г. № 212 "Вопросы Государственной технической комиссии при Президенте Российской Федерации"; Указ Президента Российской Федерации от 17.12.97 г. № 1300 "Стратегия национальной безопасности Российской Федерации" в редакции указа Президента Российской Федерации от 10.01.2000 г. № 24; Указ Президента Российской Федерации от 06.03.97 г. № 188 "Перечень сведений конфиденциального характера".

К нормативно-методическим документам вышестоящих организаций относятся: Постановление Правительства Российской Федерации от 03.11.94 г. № 1233 "Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти"; Решение Гостехкомиссии России и ФАПСИ от 27.04.94 г. № 10 "Положение о государственном лицензировании деятельности в области защиты информации" (с дополнением); Постановление Правительства Российской Федерации от 11.04.2000 г. № 326 "О лицензировании отдельных видов деятельности"; "Сборник руководящих документов по защите информации от несанкционированного доступа" Гостехкомиссия России, Москва, 1998 г.; ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения"; ГОСТ Р 50922-96 "Защита информации. Основные термины и определения"; ГОСТ Р 51583-2000 "Порядок создания автоматизированных систем в защищенном исполнении"; ГОСТ Р 51241-98 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний"; ГОСТ 12.1.050-86 "Методы измерения шума на рабочих местах"; ГОСТ Р ИСО 7498-1-99.

Руководствуясь положениями вышеперечисленных документов Гостехкомиссия России разработала свои нормативно-методические документы. К ним относятся: ряд методик по оценке защищенности основных технических средств и систем; защищённости информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации; защищенности помещений от утечки речевой информации по акустическому и виброакустическому каналам; по каналам электроакустических преобразований. Приняты: Решение Гостехкомиссии России от 14.03.95 г. № 32 "Типовое положение о Совете (Технической комиссии) министерства, ведомства, органа государственной власти субъекта Российской Федерации по защите информации от иностранных технических разведок и от ее утечки по техническим каналам"; Решение Гостехкомиссии России от 03.10.95 г. № 42 "Типовые требования к содержанию и порядку разработки Руководства по защите информации от технических разведок и ее утечки по техническим каналам на объекте" и ряд других документов.

К руководящим документам, разрабатываемым в организациях, относятся:

- руководство (инструкция) по защите информации в организации;
- положение о подразделении организации, на которое возлагаются задачи по обеспечению безопасности информации;
- инструкции по работе с грифованными документами;
- инструкции по защите информации о конкретных изделиях.

В различных организациях эти документы могут иметь разные наименования, отличающиеся от перечисленных выше. Но сущность этих документов остается неизменной, так как их наличие в организации объективно.

Руководство должно состоять из следующих разделов:

- общие положения;
- охраняемые сведения об объекте;
- демаскирующие признаки объекта и технические каналы утечки информации;
- оценка возможностей технических разведок и других источников угроз безопасности информации (возможно, спецтехника, используемая преступными группировками);
- организационные и технические мероприятия по защите информации;
- оповещение о ведении разведки (раздел включается в состав Руководства при необходимости);
- обязанности и права должностных лиц;
- планирование работ по защите информации и контролю;
- контроль состояния защиты информации;
- аттестование рабочих мест;
- взаимодействие с другими предприятиями (учреждениями, организациями).

Созданию каждого изделия или самостоятельного документа сопутствует свой набор информационных элементов, их источников и носителей, угроз и каналов утечки информации, проявляющихся в различные моменты времени.

Для защиты информации об изделии на каждом этапе его создания должна разрабатываться соответствующая инструкция. Инструкция должна содержать необходимые для обеспечения безопасности информации сведения, в том числе: общие сведения о наименовании образца, защищаемые сведения и демаскирующие признаки, потенциальные угрозы безопасности информации, замысел и меры по защите, порядок контроля (задачи, органы контроля, имеющие право на проверку, средства контроля, допустимые значения контролируемых параметров, условия и методики, периодичность и виды контроля), фамилии лиц, ответственных за безопасность информации.

Основным нормативным документом при организации защиты информации является перечень сведений, составляющих государственную, военную, коммерческую или любую другую тайну. Перечень сведений, содержащих государственную тайну, основывается на положениях закона "О государственной тайне". Перечни подлежащих защите сведений, изложенных в этом законе, конкретизируются ведомствами применительно к тематике конкретных организаций.

Перечни сведений, составляющих коммерческую тайну, составляются руководством фирмы при участии сотрудников службы безопасности.

Лабораторный практикум. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Володин Сергей Михайлович
К.т.н., доцент кафедры
Информационные системы и технологии

Цель работы:

научиться определять угрозы информационной безопасности.

Теоретические вопросы:

1. Предмет и задачи технической защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности.
3. Системный подход при решении задач инженерно-технической защиты информации.
4. Основные параметры системы защиты информации.
5. Задачи и требования к способам и средствам защиты информации техническими средствами.
6. Принципы системного анализа проблем инженерно-технической защиты информации.
7. Классификация способов и средств защиты информации.
8. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.

Задание 1. Приведите примеры воздействия на защищаемую информацию со стороны людей.

Задание 2. Опишите способы непосредственного воздействия на носители защищаемой информации.

Задание 3. Опишите пути несанкционированного распространения конфиденциальной информации.

Задание 4. Приведите способы вывода из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Задание 5. Опишите способы нарушения режима работы технических средств отображения, хранения, обработки, воспроизведения, передачи информации, средств связи и технологии обработки информации.

Задание 6. Приведите способы вывода из строя и нарушения режима работы систем обеспечения, функционирования технических средств отображения, хранения, обработки, воспроизведения и передачи информации.

Задание 7. Опишите виды дестабилизирующего воздействия на защищаемую информацию со стороны источника воздействия – технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.

Задание 8. Заполните таблицу.

Приоритет	Вид угрозы	Субъект угрозы			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
1	Травмы и гибель людей				
2	Повреждение оборудования, техники				
3	Повреждение системы жизнеобеспечения				
4	Несанкционированное изменение технологического процесса				

Приоритет	Вид угрозы	Субъект угрозы			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
	нерегламентированных технических и программных средств				
6	Дезорганизация функционирования предприятия				
7	Хищение материальных носителей				
8	Уничтожение или перехват данных путем хищения носителей				

Приоритет	Вид угрозы	Субъект угрозы			
		Стихия	Нарушитель	Злоумышленник	
				На территории	Вне территории
9	Устное разглашение конфиденциальной информации				
10	Несанкционированный съем информации				
11	Нарушение правил эксплуатации средств защиты				

Лабораторный практикум.
ОРГАНИЗАЦИЯ АТТЕСТАЦИИ ВЫДЕЛЕННОГО ПОМЕЩЕНИЯ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Володин Сергей Михайлович
К.т.н., доцент кафедры
Информационные системы и технологии

Цель:

научиться проводить аттестацию выделенного помещения по требованиям безопасности информации.

Теоретические вопросы

1. Предмет и задачи технической защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности.
3. Системный подход при решении задач инженерно-технической защиты информации.
4. Основные параметры системы защиты информации.
5. Задачи и требования к способам и средствам защиты информации техническими средствами.
6. Принципы системного анализа проблем инженерно-технической защиты информации.
7. Классификация способов и средств защиты информации.
8. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.

Задание 1. Составить самостоятельно документацию на контролируемое помещение, изучить ее, определить возможные разведопасные направления и возможные виды разведки.

Исходные данные Представитель ОАО «ХХХ», как представитель Заказчика, представил следующие исходные данные на исследуемое помещение:

1. Атрибуты объекта – ОАО «ХХХ», г. С-Петербург, ул. Строителей, дом №.., расположено на первом этаже 3-этажного здания. На 2 и 3 этажах расположены сторонние организации. Имеется общая охраняемая территория. Допуск посторонних лиц и автомашин только с согласия руководителя ОАО «ХХХ» и руководителей сторонних организаций. Все сотрудники ОАО «ХХХ» имеют допуск не ниже третьего. Сторонние организации с гостайной не работают. В ОАО «ХХХ» имеется одно выделенное помещение (ВП) – кабинет руководителя. Планируется аттестовать в качестве выделенного помещения – помещение для переговоров.

2. Контролируемая зона (КЗ) объекта проходит по ограждающим конструкциям третьего этажа, за исключением лестницы на верхние этажи. Исследуемое ВП – переговорная – граничит с КЗ по одной стене, на которой расположены одно окно и дверь, и по потолку. Средства звукоусиления в переговорной отсутствуют. Источник речи не локализован.

3. Помещению планируется установить вторую категорию.

4. Граничащие помещения (спереди, сзади, справа, слева, снизу, сверху).

5. Ограждающие конструкции: Стены 1 и 2 выполнены из кирпича. Толщина 2,5 кирпича. Внутренняя штукатурка толщиной 1 см. Боковые стены 3 и 4 выполнены из кирпича. Толщина 1 кирпич. Внутри и снаружи штукатурка толщиной 1 см. Пол и потолок выполнены из стандартных бетонных плит перекрытия толщиной 30 см. Подвала нет. Сквозных щелей и пустот не обнаружено. Пол деревянный на лагах, покрыт линолеумом. Фальшпотолка нет.

6. Двери двойные с тамбуром. Ширина тамбура – 0,5 м. По периметру каждой двери проложен уплотнитель. Двери тяжелые деревянные. Дверные коробки отделены друг от друга и от стены резиновыми уплотнителями. Дверь выходит на границу КЗ.

7. Окно пластиковое в специальном исполнении. Рама окна отделена от стены резиновыми прокладками. Окно граничит с КЗ.

8. В помещении имеется одна батарея отопления. Трубы системы отопления выполнены из металлопластика. Ввод трубы системы отопления осуществлен со второго этажа, выход трубы идет под пол. Тепловой пункт размещен за пределами КЗ. Таким образом, система отопления имеет выход за пределы КЗ.

9. Система вентиляции выполнена в виде вентиляционных коробов и имеет ближайший выход в общий коридор первого этажа и затем выходит на второй и третий этаж (по легенде).

10. На элементах ограждающих конструкций и инженерных коммуникаций имеются средства активной защиты.

Задание 2. Изобразить план-схему исследуемого помещения.

Задание 3. На основании нижеприведенной методики составить план проведения визуального осмотра помещения и выявить объекты, требующие при обследовании использования имеющихся средств видеонаблюдения.

Задание 4. Сделать выводы по результатам проделанной работы и подготовить отчет.

3.6. Оценить устойчивость каждой фирмы-разработчика ИС (т.е. определить время существования их на рынке; определить долю занимаемого рынка; наличие сети сертифицированных центров технической поддержки; авторизованных учебных центров; "горячих линий" для консультаций и т.д.).

3.7. Оценить преимущества и недостатки каждой фирмы, сопоставив полученные данные, и выбрать наиболее подходящую фирму-разработчика ИС по выделенным критериям.

Лабораторный практикум. ИЗМЕРЕНИЕ ПАРАМЕТРОВ ФИЗИЧЕСКИХ ПОЛЕЙ

Володин Сергей Михайлович

К.т.н., доцент кафедры Информационные системы и технологии

Цель:

изучить основные параметры физических полей.

Теоретические вопросы

1. Понятие физического поля.
2. Понятие и параметры электромагнитного поля.
3. Понятия и параметры акустического, виброакустического, гидроакустического полей.

Задание 1. Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения.

Задание 2. В чем отличие электростатического поля от вихревого электрического поля? Какому закону подчиняется взаимодействие неподвижных электрических зарядов?

Задание 3. Что является источником магнитных полей? Приведите примеры магнитных полей в природе. Перечислите свойства линий магнитной индукции. В каких случаях магнитное поле называется однородным?

Задание 4. Какими существенными свойствами отличается магнитное поле от электрического?

Задание 5. Назовите характеристики электрического поля и их единицы измерения.

Задание 6. Назовите характеристики магнитного поля и их единицы измерения.

Задание 7. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля?

Задание 8. Как изменяются векторы напряженности электрического и магнитного поля в ближней зоне? Как изменяются векторы напряженности электрического и магнитного поля в дальней зоне?

Задание 9. Что такое акустическое поле? На какие виды оно подразделяется?

Лабораторный практикум. ЗАЩИТА ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

Володин Сергей Михайлович
К.т.н., доцент кафедры
Информационные системы и технологии

Цель:

изучить способы защиты информации от утечки по акустическому каналу.

Теоретические вопросы

1. Понятие звуковой волны.
2. Характеристики звуковых волн.
3. Акустический (речевой) канал.
4. Способы съема акустической информации.
5. Сила (интенсивность) звука.
6. Звукоизоляция стен и сплошных перегородок.
7. Средства могут использоваться для защиты информации от утечки по акустическому каналу.

Задание 1. Что изучает акустика? Какие понятия определяет слово звук?

Задание 2. В чем заключается основное отличие акустических волн от электромагнитных?

Задание 3. Почему акустический канал утечки информации является наиболее распространенным?

Задание 4. Для защиты речевой информации ограниченного доступа при проведении переговоров компания, арендующая свои производственные площади, использует специальное помещение – защищённый служебный кабинет (ЗСК). Двери и окна ЗСК надёжно защищены от прослушивания техническими средствами защиты информации. Однако кирпичная перегородка, отделяющая ЗСК от незащищённого коридора, не арендуемого компанией и допускающего возможность проникновения в него злоумышленников, имеет толщину всего в полкирпича. Размеры перегородки 10 × 3 м. Размеры одинарного силикатного кирпича по СТБ 1160-99 «Кирпич и камни керамические. Технические условия» составляют 250 × 120 × 65 мм. Используя данные таблицы, определить стоимость дополнительной кирпичной кладки, усиливающей звукоизоляцию стены для обеспечения затухания Q информационного сигнала в стене на частоте 1000 Гц до уровня не менее: – 58 дБ – для варианта 1; – 61 дБ – для варианта 2; – 65 дБ – для варианта 3; – 67 дБ – для варианта 3 при стоимости кирпича 250 $ за кубометр и при стоимости кирпичной кладки 25 $ за кубометр. Толщиной швов между кирпичами, потерями кирпича на бой и другие цели, стоимостью других работ и материалов при усилении звукоизоляции стены в первом приближении пренебречь.

Вид конструкции	Толщина конструкции	Среднее значение Q, дБ, для среднегеометрической частоты, Гц				
		50	500	1000	2000	4000
Кирпичная кладка, оштукатуренная с двух сторон	0,5 кирпича 1 кирпич 1,5 кирпича 2 кирпича 2,5 кирпича	40 44 48 52 55	42 51 55 59 60	48 58 61 65 67	54 64 65 70 70	60 65 65 70 70
Железобетонная панель	100мм 160 мм 300мм 400мм	40 47 50 55	44 51 58 61	50 60 65 67	55 63 65 70	60 63 65 70
Гипсобетонная панель	86 мм	33	39	47	54	60
Керамзитобетонная панель	80мм 120мм 140мм	34 37 43	39 39 47	47 47 53	52 54 57	60 51 61
Шлакоблоки, оштукатуренные с двух сторон	220мм	42	48	54	60	63
Древесностружечная плита	30 мм	26	26	26	26	26

Задание 5. Определить для своего варианта задания 1, во сколько раз сила звука в коридоре при использовании обсчитанного вами варианта кирпичной кладки будет больше или меньше при установке не кирпичной перегородки, а перегородки из материала: – железобетонная панель, толщина 100 мм – вариант 1; – гипсобетонная панель, толщина 86 мм – вариант 2; – шлакоблоки, толщина 220 мм – вариант 3; – древесностружечная плита (ДСП), толщина 30 мм – вариант 4.

Лабораторный практикум. СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ПРОВОДНОМУ КАНАЛУ

Володин Сергей Михайлович
К.т.н., доцент кафедры
Информационные системы и технологии

Цель:

изучить технические средства защиты от утечки информации по проводному каналу.

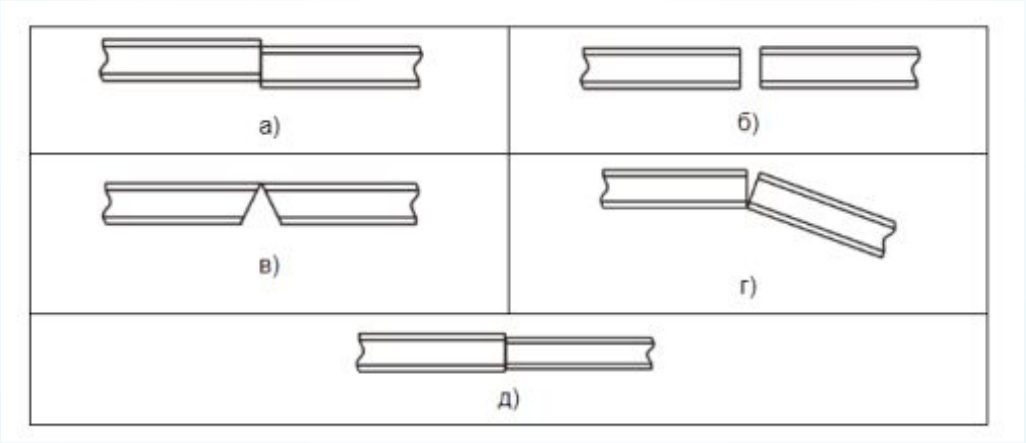
Теоретические вопросы

1. Технические каналы утечки информации, передаваемой по каналам проводной связи.
2. 2. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.

Задание 1. Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей.

Задание 2. Приведите основные причины утечки информации в волоконно-оптических линиях.

Задание 3. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон:



Задание 4. Заполните таблицу.

Взаимное влияние различных типов линий и меры их защиты

Тип линии	Преобладающее влияние	Меры защиты
Воздушные линии связи		
Коаксиальный кабель		
Симметричный кабель		
Оптический кабель		

Лабораторный практикум. ЗАЩИТА ОТ УТЕЧКИ ПО ВИБРОАКУСТИЧЕСКОМУ КАНАЛУ

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

Цель:

изучить средства защиты информации от утечки по виброакустическому каналу.

Теоретические вопросы

1. Понятие виброакустического канала утечки информации.
2. Методы и средства защиты речевой информации от утечки по виброакустическому каналам.
3. Генераторы виброакустического шума.
4. Приборы виброакустической защиты.

Задание 1. Что представляет собой речевой тракт человека? На основании чего определяется тип человеческого голоса?

Задание 2. Что является основой анализа разборчивости речевой информации? Каков диапазон уровней человеческой речи? Какие звуки являются наиболее информативными с точки зрения разборчивости речевой информации?

Задание 3. На каком расстоянии от источника производится измерение уровней речи?

Задание 4. Что используют для количественной оценки качества перехваченной речевой информации?

Задание 5. Какова шкала оценок качества перехваченного речевого сообщения?

Задание 6. При каком уровне словесной разборчивости будет наблюдаться срыв связи? Какой уровень словесной разборчивости нужен для составления подробной справки о содержании перехваченного разговора?

Задание 7. Для какого уровня словесной разборчивости уже непригодны приборы техники фильтрации помех?

Задание 8. Опишите структурную схему виброакустического канала

Задание 9. Изучите принцип действия прибора виброакустической защиты SI-3001.

Задание 10. Изучите принцип действия прибора “PTRD-018” – стационарного обнаружителя диктофонов.

Лабораторный практикум. ОПРЕДЕЛЕНИЕ КАНАЛОВ УТЕЧКИ ПЭМИН

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

Цель:

определение каналов утечки ПЭМИН.

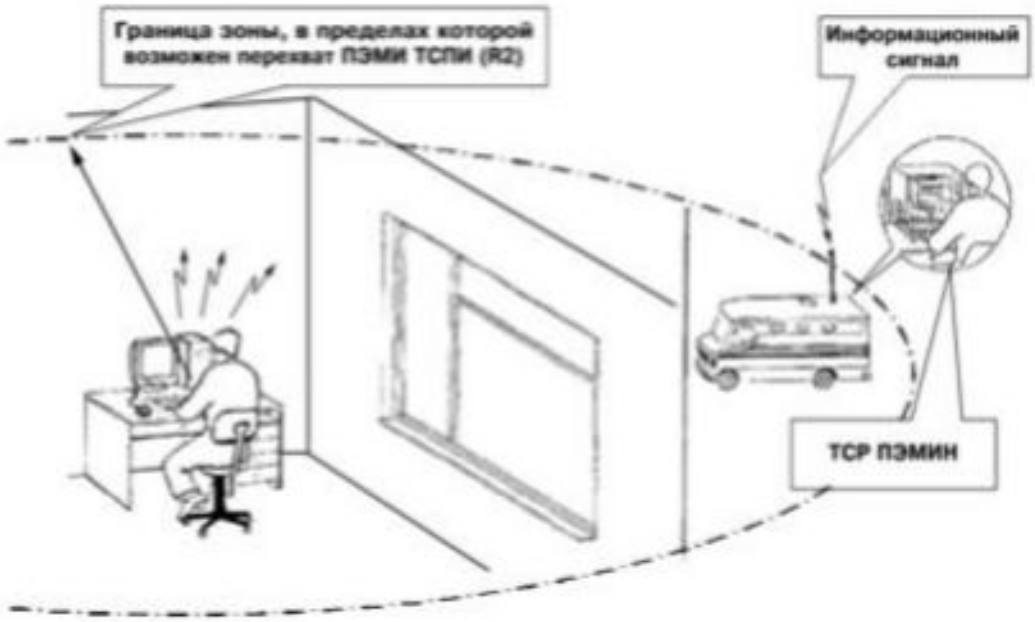
Теоретические вопросы

1. Технические средства передачи, обработки, информации ограниченного доступа (ТСПИ).
2. Состав ТСПИ.
3. Побочные электромагнитные излучения элементов ТСПИ.
4. Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ.
5. Побочные электромагнитные генерации в элементах ТСПИ.
6. Перехват побочных электромагнитных излучений ТСПИ.
7. Методы защиты информации от ПЭМИН.

Задание 1. Опишите схему технического канала утечки информации.

Задание 2. Опишите способы перехвата побочных электромагнитных излучений ТСПИ.

Перехват побочных электромагнитных излучений ТСПИ средствами разведки ПЭМИН



Задание 3. Изучите принцип действия программно-аппаратного комплекса «НАВИГАТОРПЗГ».

Задание 4. Опишите технологию исследования ПЭМИН-монитора

Лабораторный практикум. ЗАЩИТА ОТ УТЕЧКИ ПО ЦЕПЯМ ЭЛЕКТРОПИТАНИЯ И ЗАЗЕМЛЕНИЯ

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

Цель:

проанализировать разные философские взгляды на роль личности в истории.

Теоретические вопросы

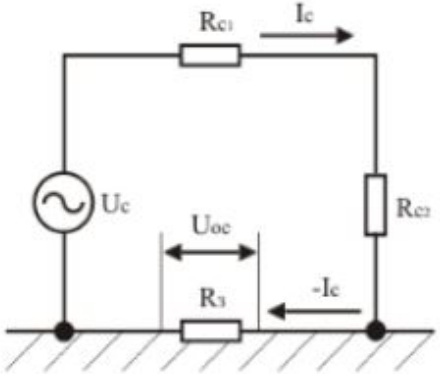
1. Защита информации от утечки по цепям заземления.

2. Защита информации от утечки по цепям электропитания.

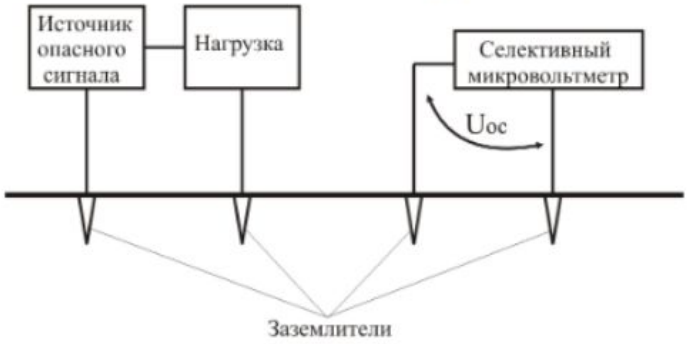
3. Подавление опасных сигналов. Источники опасных сигналов.

Задание 1. Опишите варианты утечки информации по цепям заземления (рисунок 1).

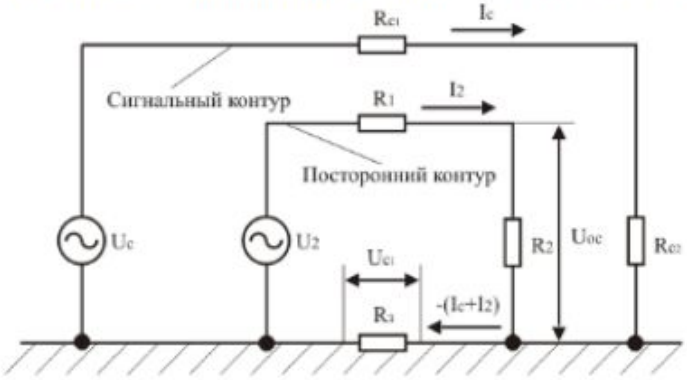
Утечка информации за счет падения напряжения на сопротивлении заземляющего устройства



Утечка информации по цепям заземления, обусловленная наличие электромагнитного поля в грунте

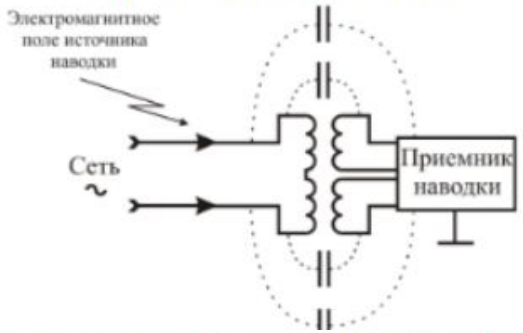


Утечка информации по общей цепи заземления двух различных устройств

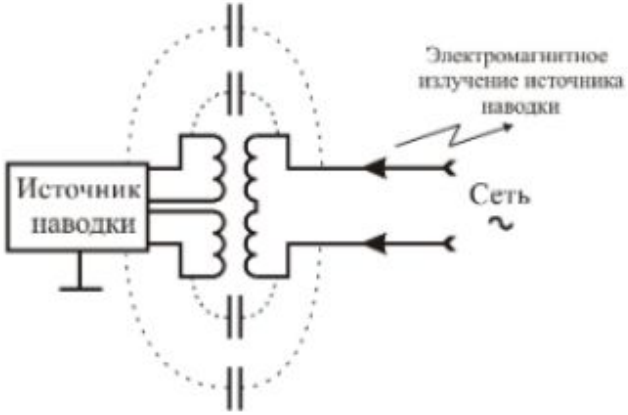


Задание 2. Опишите варианты утечки информации по цепям электропитания (рисунок 2).

Утечка информации по цепям электропитания за счет побочных электромагнитных наводок



Утечка информации по цепям электропитания за счет побочного электромагнитного излучения



Задание 3. Опишите меры по предотвращению утечки защищаемой информации по цепям заземления.

Задание 4. Опишите меры по предотвращению утечки защищаемой информации по цепям электропитания.

Задание 5. Изучите принцип действия прибора РНИ-1.1.

Лабораторный практикум. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕФОННЫХ ЛИНИЯХ

Володин Сергей Михайлович
К.т.н., доцент кафедры
Информационные системы и технологии

Цель:

изучить технические средства защиты информации в телефонных линиях.

Теоретические вопросы

1. Способы защиты информации от прослушивания.
2. Структурное скрытие речевой информации в каналах связи.
3. Обнаружение и подавление закладных устройств.
4. Определение подключений к телефонным линиям средств кражи информации.
5. Технические средства защиты информации в телефонных линиях.

Задание 1. Назовите и охарактеризуйте пассивные технические средства защиты телефонной линии. Заполните таблицу.

Ограничения опасных сигналов		
Фильтрация опасных сигналов		
Отключение преобразователей (источников) опасных сигналов		

Задание 2. Контроль состояния телефонной линии и обнаружение атак осуществляется посредством применения аппаратуры контроля линий связи. Охарактеризуйте устройства.

Телефонный анализатор	
Рефлектометр (или «кабельный радар»)	

Задание 3. Опишите методы активной защиты информации в телефонных линиях

Подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи)	
Подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи)	
Подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи)	
Поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения)	
Подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод "обнуления")	
Подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи)	
Подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод)	
Подача в телефонную линию высоковольтных импульсов (метод "выжигания")	

Лабораторный практикум. СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ЭЛЕКТРОСЕТЕВОМУ КАНАЛУ

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

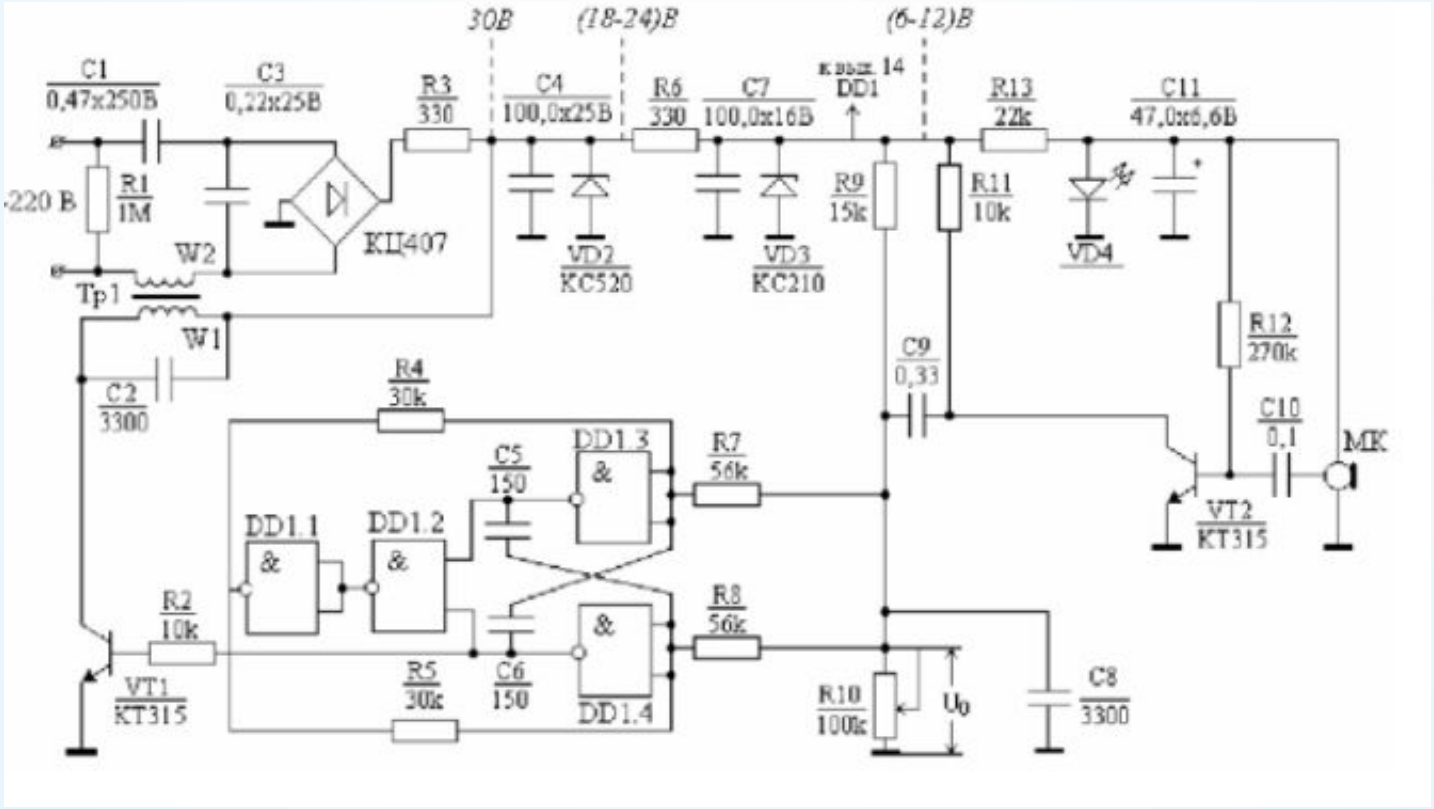
Цель:

изучить технические средства защиты информации от утечки по электросетевому каналу.

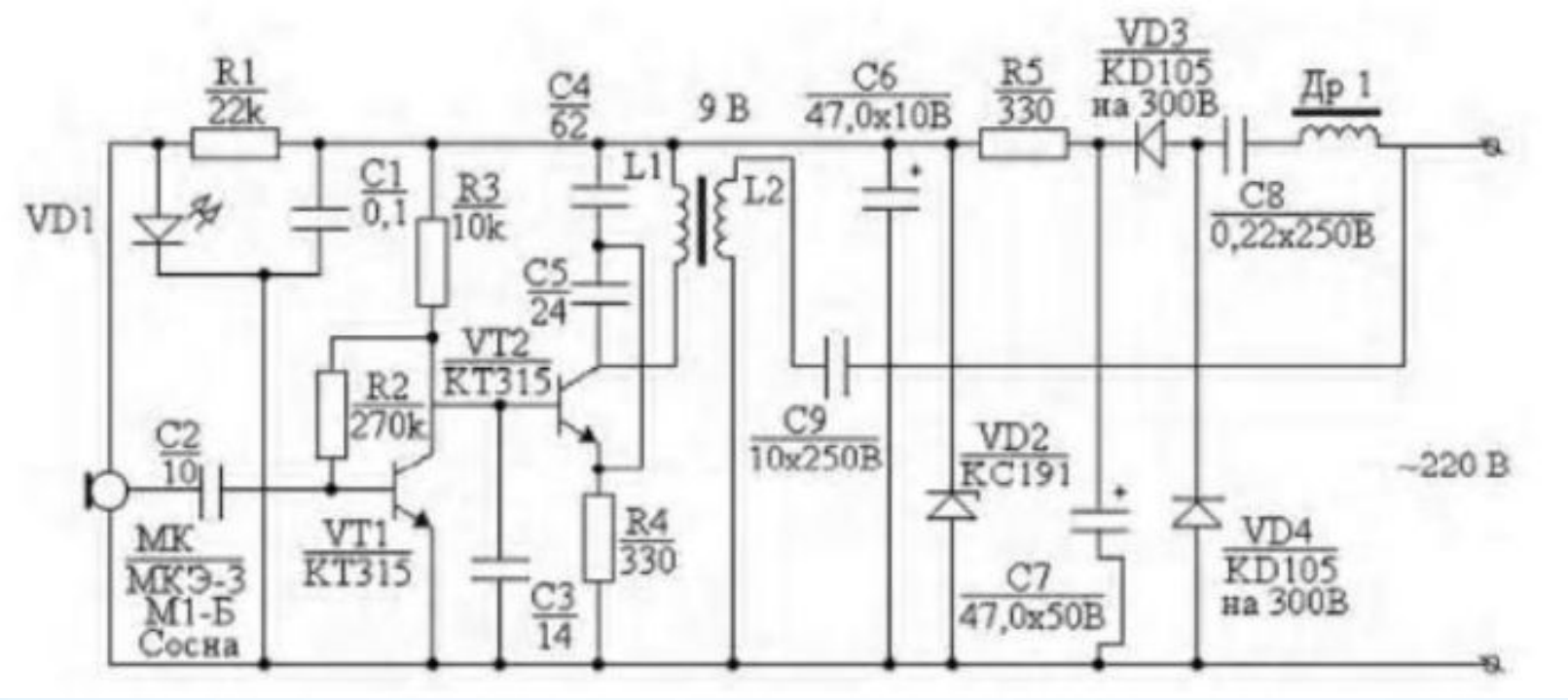
Теоретические вопросы

1. Особенности передачи сигнала по электросетевому каналу.
2. Электросетевые закладки.
3. Низкочастотное устройство съема информации.
4. Высокочастотное устройство съёма информации.
5. Системы защиты от утечки по электросетевому каналу.

Задание 1. Опишите принципы работы низкочастотного устройства съема информации, состоящего из блока питания, предварительного усилителя сигнала с микрофона, генератора и усилителя мощности (рисунок 3).



Задание 2. Опишите принципы работы высокочастотного устройства съема информации.



Задание 3. Опишите методы подавления опасных сигналов.

Задание 4. Опишите системы защиты от утечки по электросетевому каналу.

Лабораторный практикум. СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ОПТИЧЕСКОМУ КАНАЛУ

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

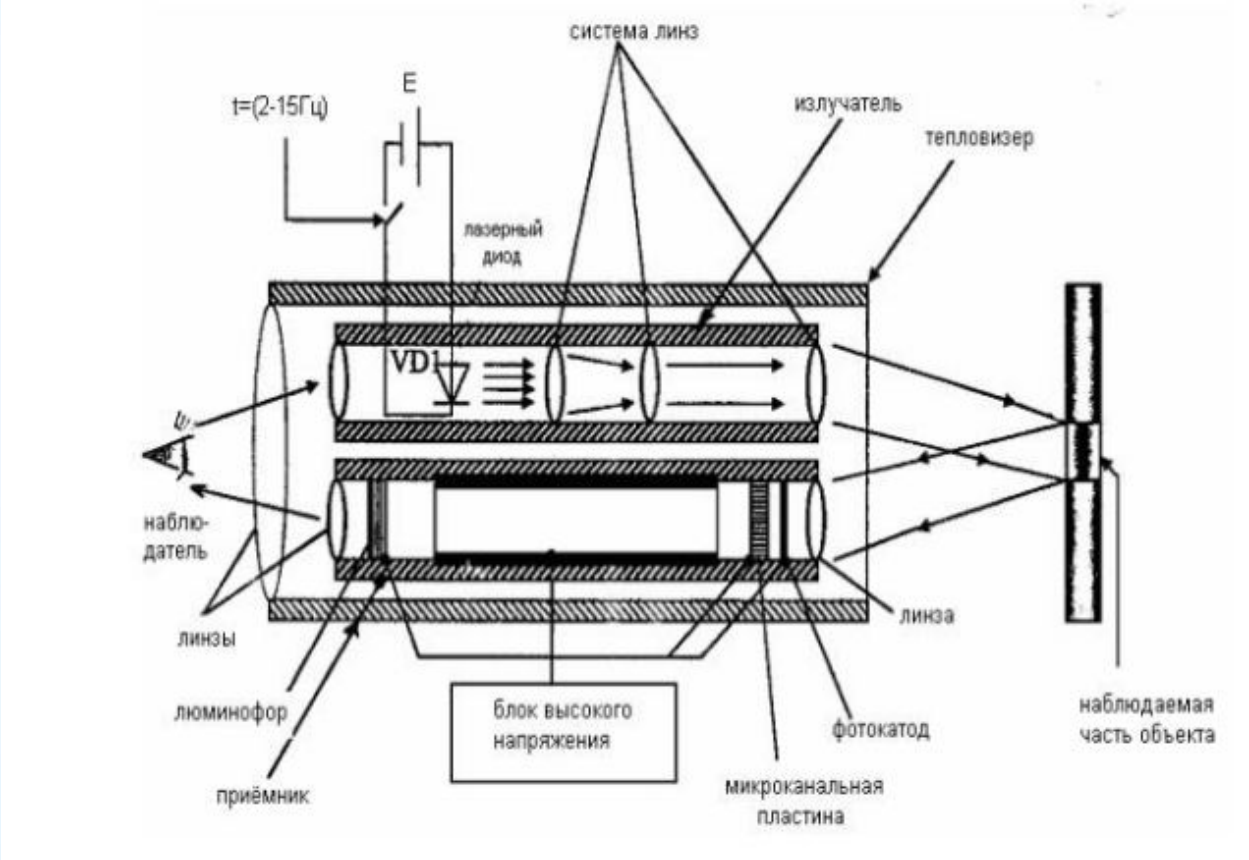
Цель:

изучить системы защиты от утечки информации по оптическому каналу.

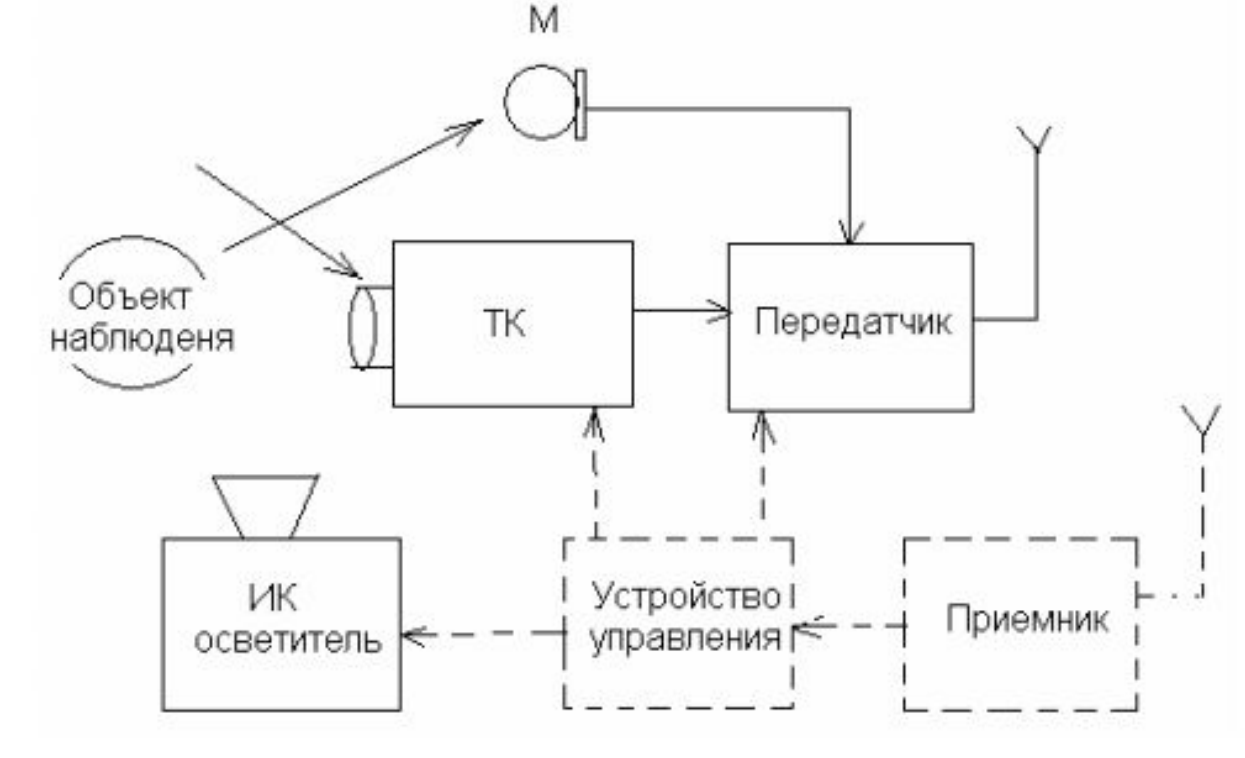
Теоретические вопросы

1. Оптический канал утечки информации.
2. Способы получения информации в оптическом канале.
3. Среды распространения в оптическом канале утечки информации.

Задание 1. Опишите технологию работы приборов ночного видения. Приведите недостатки приборов ночного видения.



Задание 2. Опишите технологию работы телевизионных систем наблюдения



Задание 3. Опишите оптические каналы утечки информации:

• объект наблюдения в кабинете – окно кабинета – окно противоположного дома – оптический прибор злоумышленника;

• объект наблюдения в кабинете – приоткрытая дверь – злоумышленник;

• объект наблюдения в кабинете – телевизионное закладное устройство – проводной или радиоканал – телевизионный приемник злоумышленника.

Задание 4. Опишите структурную модель оптических каналов утечки информации.

Источник информации	Путь утечки информации	Вид канала	Длина канала	Риск утечки	Величина ущерба	Ранг угрозы

Лабораторный практикум. ПРИМЕНЕНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

Цель:

изучить технические средства защиты информации.

Теоретические вопросы

1. Технические средства для уничтожения информации и носителей информации, порядок применения.
2. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.
3. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.
4. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

Задание 1. Приведите примеры каналов утечки информации.

Задание 2. Опишите средства защиты информации от утечки по визуально-оптическим каналам.

Задание 3. Опишите средства защиты информации от утечки по акустическим каналам.

Задание 4. Опишите средства защиты информации от утечки по электромагнитным каналам.

Задание 5. Опишите средства защиты информации от утечки по материально-вещественным каналам.

Лабораторный практикум. ЭКСПЛУАТАЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Володин Сергей Михайлович
К.т.н., доцент кафедры Информационные системы и технологии

Цель:

изучить технические средства защиты информации.

Теоретические вопросы

1. Этапы эксплуатации технических средств защиты информации.
2. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.
3. Установка и настройка технических средств защиты информации.
4. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
5. Организация ремонта технических средств защиты информации.
6. Проведение аттестации объектов информатизации.

Задание 1. Заполните таблицу.

№ п/п	Наименование оборудования и технических средств	Виды работ, при которых используется оборудование и технические средства
1	Комплект досмотровых зеркал (ПОИСК-2, ШМЕЛЬ-2)	
2	Комплект луп, фонерей	
3	Технический эндоскоп с дистальным концом (серия ЭТ, Olimpus)	
4	Комплект отверток, ключей и радиомонтажного инструмента	
5	Досмотровый металлоискатель (УНИСКАН 7215, АКА 7202, Comet)	
6	Переносная рентгенотелевизионная установка (ШМЕЛЬ 90/К, ФП-1, РОНА)	

№ п/п	Наименование оборудования и технических средств	Виды работ, при которых используется оборудование и технические средства
8	Переносный радиоприемник или магнитола	
9	Многофункциональный поисковый прибор (ПИРИНЬЯ, ПСЧ-5, D-088)	
10	Низкочастотный нелинейный детектор проводных коммуникаций (ВИЗИР, возможна замена по телефонным линиям: ТПУ-6 или SELSP-18/T)	
11	Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-600М, КРК, АРК-Д1, OSC-5000)	
12	Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов)	

№ п/п	Наименование оборудования и технических средств	Виды работ, при которых используется оборудование и технические средства
13	Дозиметр поисковый (РМ-1401, НПО-3)	
14	Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НАВИГАТОР, ЛЕГЕНДА, ЗАРНИЦА)	
15	Комплекс для проведения акустических и виброакустических изменений (СПРУТ-4А)	

Задание 2. Для одного из технического средства защиты информации опишите порядок установки, настройки и диагностики.