СМОЛЕНСКАЯ АКАДЕМИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

И. А. Ромашкова

РАБОЧАЯ ТЕТРАДЬ ПО МДК.03.01. ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА, ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

специальности 10.02.01,

МДК.04.03. ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

специальности 09.02.01

Смоленск

2020

Рабочая тетрадь по междисциплинарным курсам для специальности 10.02.01 *Организация и технология защиты информации* (базовой подготовки) *Технические методы и средства, технологии защиты информации* и студентов специальности 09.02.01 *Компьютерные системы и комплексы* (углубленной подготовки).

Составитель: Ромашкова И.А. – Смоленск: ОГБПОУ СмолАПО, 2020.

СОДЕРЖАНИЕ

Пояснительная записка

Представленные материалы разработаны на основе рабочей программы профессионального модуля ПМ.03 *Программно-аппаратные и технические средства защиты информации* и предназначены для студентов специальности 10.02.01 *Организация и технология защиты информации* базовой подготовки и рабочей программы профессионального модуля ПМ.04 *Разработка компьютерных систем и комплексов* специальности 09.02.01 Компьютерные системы и комплексы.

Разработка имеет своей целью методическое сопровождение самостоятельной работы студентов по МДК.03.01. *Технические методы и средства, технологии защиты информации* и МДК.04.03. *Технические методы и средства защиты информации*. Рабочая тетрадь ориентирована на формирование умений организовывать собственную деятельность; выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество; осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, использовать информационно-коммуникационные технологии в профессиональной деятельности, ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

Методические указания

Отчет к практическому занятию оформляется в рабочей тетради и в электронном документе, который сохраняется на своем носителе или ресурсе, указанном преподавателем.

Каждый из документов содержит название и цель, в электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы. Требования к оформлению отчета и электронного документа перечислены в ПРИЛОЖЕНИИ А.

Ответы на задания даются полные, в соответствие с вопросом. При работе с нормативно-правовыми документами указывается название документа, на

который ссылается обучающийся. В качестве источников законодательных актов необходимо использовать справочно-правовые системы КонсультантПлюс, Гарант, официальные сайты организаций и структур.

Практическое занятие 1
Законодательная и нормативная база правового регулирования вопросов технической защиты информации

Цель: анализ системы нормативных правовых актов по технической защите информации.

Задание 1. Дайте ответы на вопросы.

1. Объектами технической защиты информации (ТЗИ) могут быть:_____

_____

_____

_____

2. Доктрина информационной безопасности РФ отображает _____

_____

_____

3. Нормативные правовые акты по технической защите информации – ____

_____

_____

5. Организационные документы – _____

_____

6. Государственные стандарты – _____

_____

_____

_____

7. Руководящие документы – _____

_____

_____

Задание 2. Составьте перечень основных правоустанавливающие документов, связанных с технической защитой информации **(**ФЗ, стандарты, руководящие документы, постановления правительства и т.п.).

Указание. Перечень сохранятся в электронном документе под названием *Основные правоустанавливающие документы по ТехЗ.*

Контрольные вопросы

1. Назовите основные виды конфиденциальной информации.
2. Назовите интересы государства в области обеспечения информационной безопасности.
3. В каком законе приведена классификация средств защиты информации?
4. Назовите основные положения Доктрины информационной безопасности РФ.
5. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://fstec.ru/
4. Сайт Федерального агентства по метрологии. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.gost.ru/wps/portal/

Практическое занятие 2
Задачи и функции органов по технической защите информации в РФ

Цель: анализ структуры и функций государственного аппарата обеспечения информационной безопасности РФ; анализ задач и функций органов по технической защите информации в РФ.

Задание 1. Охарактеризуйте систему государственного регулирования и контроля в области информационной безопасности РФ.

Методические рекомендации. Характеристику оформите в виде таблицы в тетради для практических занятий, отразите название специальных государственных органов и структур, кто руководит этими органами, кому подчиняются, дайте их определение.

Задание 2. Дайте ответы на вопросы, продолжите фразы:

1. ФСБ РФ в области технической защиты информации отвечает за _____

_____

_____

2. Когда создана ФСТЭК? На месте, какого государственного органа?_____

_____

3. Укажите документ, в котором описаны основные цели, задачи и функции ФСБ (названия, дата утверждения, последние изменения).

_____

_____

_____

4. Укажите документ, в котором описаны основные цели, задачи и функции ФСТЭК (названия, дата утверждения, последние изменения).

_____

_____

_____

Задание 3. В электронном документе под названием *Органы_ТЗ_РФ* дайте ответы на вопросы:

1. Каковы основные задачи ФСБ, связанные с технической защитой информации (по документу из вопроса 3 задания 2)?

2. Каковы основные функции ФСБ, связанные с технической защитой информации (по документу из вопроса 3 задания 2)?

3. Каковы основные задачи ФСТЭК (по документу из вопроса 4 задания 2)?

Контрольные вопросы

1. Перечислите органы государственного регулирования и контроля в области информационной безопасности РФ.
2. Назовите документы, которым руководствуется ФСБ России в своей деятельности?
3. Перечислите основные задачи и функции ФСБ в области технической защиты информации.
4. Перечислите основные задачи и функции ФСТЭК в области технической защиты информации. Каковы полномочия ФСТЭК?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
5. Сайт Федеральной службы безопасности РФ. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fsb.ru/

Практическое занятие 3
Лицензирование деятельности в области защиты информации

Цель: анализ положений о государственном лицензировании деятельности в области защиты информации.

Задание 1. Проанализируйте положения №99-ФЗ «О лицензировании отдельных видов деятельности» и дайте ответы на следующие вопросы.

1. Сфера деятельности настоящего закона_____

_____

_____

_____

2. Положения настоящего Федерального закона не применяются к отношениям, связанным с осуществлением лицензирования (в области защиты информации) _____

_____

4. ***Лицензия*** – это _____

_____

_____

_____

_____

6. ***Лицензионные требования*** – _____

_____

_____

_____

7. Лицензия выдается (срок)_____

_____

7. Действие лицензии приостанавливается лицензирующим органом в следующих случаях_____

_____

_____

_____

_____

_____

_____

8. Сведения о приостановлении действия лицензии вносятся _____

_____

9. За исключением, каких случаев информация по вопросам лицензирования (в том числе сведения, содержащиеся в реестрах лицензий) является открытой?

_____

_____

_____

Задание 2. Проанализируйте положения №99-ФЗ «О лицензировании отдельных видов деятельности» и выполните задания, сохранив их в файл под именем *Лицензирование.*

1. Составьте список лицензионных требований.
2. Составьте перечень оснований для отказа предоставления лицензии.
3. Составьте список сведений включаемых в реестре лицензий.
4. Сохраните в отдельные электронные документы формы:
   а) типовая форма лицензии;
   б) заявление о предоставлении лицензии.

Задание 3. Составьте перечень видов деятельности, на которые требуются лицензии в области защиты информации.

Методические рекомендации. Перечень оформите в виде таблицы, сохранив его в файл под именем *Перечень видов деятельности*, во второй колонке, указав лицензирующий орган по каждому виду деятельности.

Задание 4. Проанализируйте *Реестр лицензий на деятельность по технической защите конфиденциальной информации* на сайте ФСТЭК.

1. Составьте перечень организаций Смоленска и Смоленской области, умеющих данный вид лицензии: номер лицензии, дату выдачи лицензии, адрес организации.

Методические рекомендации. Перечень оформите в виде таблицы в электронный документ под именем *Реестр по ТЗ КИ*, оставив колонку для пункта 2.

2. На сайтах выбранных организаций проанализируйте направления их деятельности и отразите их в таблице пункта 1.

Контрольные вопросы

1. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.
2. Охарактеризуйте организационную структуру системы государственного лицензирования в области защиты информации.
3. Назовите случаи приостановления или прекращения действия лицензии.
4. В каких случаях предприятию отказывают в выдаче лицензии?
5. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?
6. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
2. Сайт Федеральной службы безопасности РФ. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fsb.ru/
3. Справочно-правовая система КонсультантПлюс.

Практическое занятие 4
Изучение общего порядка аттестации объекта информатизации по требованиям безопасности информации

Цель: изучить порядок аттестации информатизации, функции органов аттестации объекта информатизации по требованиям безопасности информации.

Задание 1. Ответьте на предложенные ниже вопросы или продолжите фразу, используя Интернет-ресурс www.intuit.ru и СПС.

1. Организация, осуществляющая деятельность по аттестации объектов информатизации по требованиям безопасности –_____

2. **Объект информатизации** – это _____

_____

_____

_____

_____

_____

Аттестация объектов информатизации – это_____

_____

_____

_____

_____

_____

3. Аттестация объектов информатизации по требованиям безопасности производится в соответствии с _____

_____

_____

3. Наличие аттестата соответствия в организации дает право _____

_____

_____

4. Аттестация является обязательной:

_____

_____

_____

_____

Аттестация является добровольной_____

_____

5. Цель аттестации_____

_____

6. К проверяемым требованиям относятся:

_____

_____

_____

_____

_____

7. Схема объекта информатизации, предоставляемая органу по аттестации включает _____

_____

_____

_____

_____

8. Аттестат соответствия выдается на период _____

_____

_____

_____

_____

_____

Задание 2. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС, выполнив задания, сохраните их в электронном документе под именем *Аттестация объектов информатизации*.

1. Каков перечень работ по аттестации?
2. В структуру системы аттестации входят...
3. Каковы функции органов по аттестации?
4. Какие функции ФСТЭК осуществляет в рамках системы аттестации?
5. Какие документы заявитель предоставляет органу по аттестации для проведения испытаний?
6. Аттестат соответствия должен содержать...

Задание 3. Проанализируйте Положение по аттестации объектов информатизации по требованиям безопасности информации и сохраните в электронный документ формы нормативной документации под именем *Документы аттестации*.

1. Заявка на проведение аттестации объекта информатизации.
2. Аттестат соответствия.

Контрольные вопросы

1. Охарактеризуйте систему аттестации объектов информатизации на соответствие требованиям по безопасности информации.
2. Что подразумевают под объектом информатизации?
3. Когда проводится аттестация объектов информатизации, и какова ее цель?
4. Каков период действия аттестата соответствия?
5. Перечислите функции ФСТЭК в рамках системы аттестации.
6. Что содержит аттестат соответствия?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.

3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/

4. Сайт Федеральной службы безопасности РФ. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fsb.ru/

5. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 5
Классификация угроз

Цель: изучить классификацию угроз; ознакомиться со способами оценки рисков; сравнить эти способы с точки зрения преимущества и недостатков.

Задание 1. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС.

1. **Автоматизированная система** (АС) – это _____

_____

_____

2. АС представляет собой совокупность следующих компонентов:

_____

_____

_____

_____

3. Базовой информацией для построения оптимальной системы защиты является _____

_____

_____

4. ***Угроза безопасности информации*** – _____

_____

_____

Угроза информационной безопасности АС – _____

_____

_____

_____

_____

Источник угрозы безопасности информации – _____

_____

_____

5. Основные источники нарушения безопасности в АС:

_____

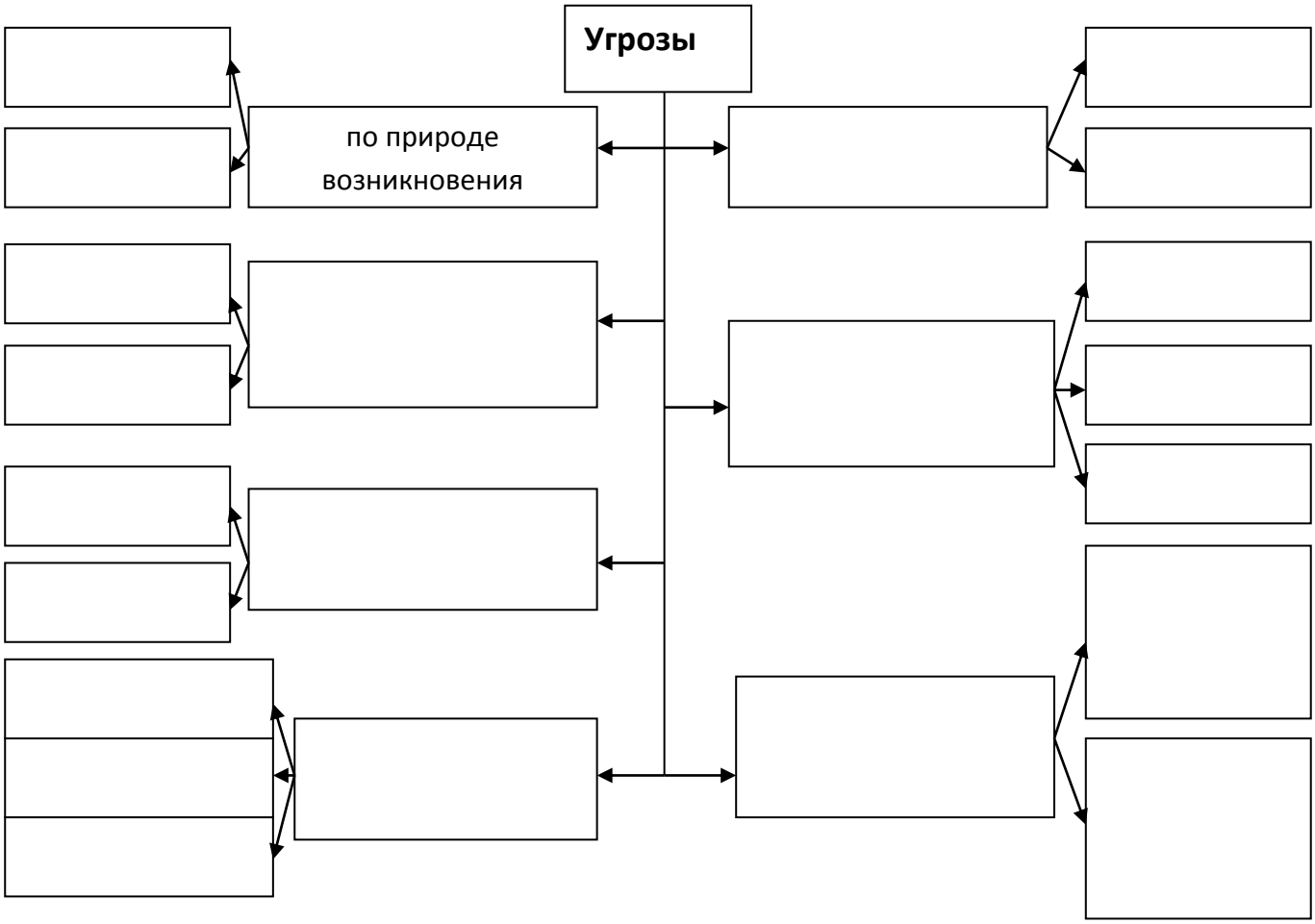
_____

_____

_____

_____

7. Составьте схему классификации угроз АС.



7. Риск – _____

_____

8. Целью количественной оценки риска является _____

_____

_____

_____

9. Результатом проведения количественного анализа является:

_____

_____

_____

_____

10. Основные факторы для оценки потенциального ущерба:

_____

_____

_____

_____

_____

Задание 2. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС, выполнив задания, сохраните их в электронном документе под именем *Угрозы*.

1. Перечислите основные случайные угрозы и основные преднамеренные угрозы**.**

2. Какими знаниями должны обладать эксперты для оценки рисков?

3. Целью количественной оценки риска является?

4. Какие характеристики и факторы предлагается учитывать по методу компании Microsoft при количественной оценке рисков?

5. Основными факторами при оценке вероятности являются ...

6. Отразите в таблице сравнение двух подходов к оценке рисков.

Контрольные вопросы

1. Что понимают под автоматизированной системой? Перечислите основные источники нарушения безопасности в АС. Дайте классификацию угроз АС.
2. Дайте характеристику классов понятий риск и ущерб.
3. Охарактеризуйте способы количественной и качественной оценки рисков.

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.

3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
4. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 6
Классификация объектов защиты

Цель: проанализировать классификацию объектов защиты; ознакомиться требованиями к классам защищенности АС и СВТ.

Задание 1. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС. В тетради для практических занятий дайте ответы на следующие вопросы.

1. ФСТЭК под объектами информатизации, аттестуемыми по требованиям безопасности информации, понимает _____

_____

_____

_____

_____

_____

2. Защищаемыми объектами информатизации в соответствии со «Специальные требования и рекомендации по технической защите конфиденциальной информации» являются:

_____

_____

_____

_____

_____

_____

_____

_____

_____

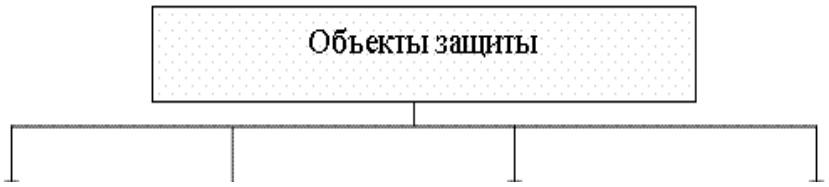
3. ***Объект защиты информации –*** _____

_____

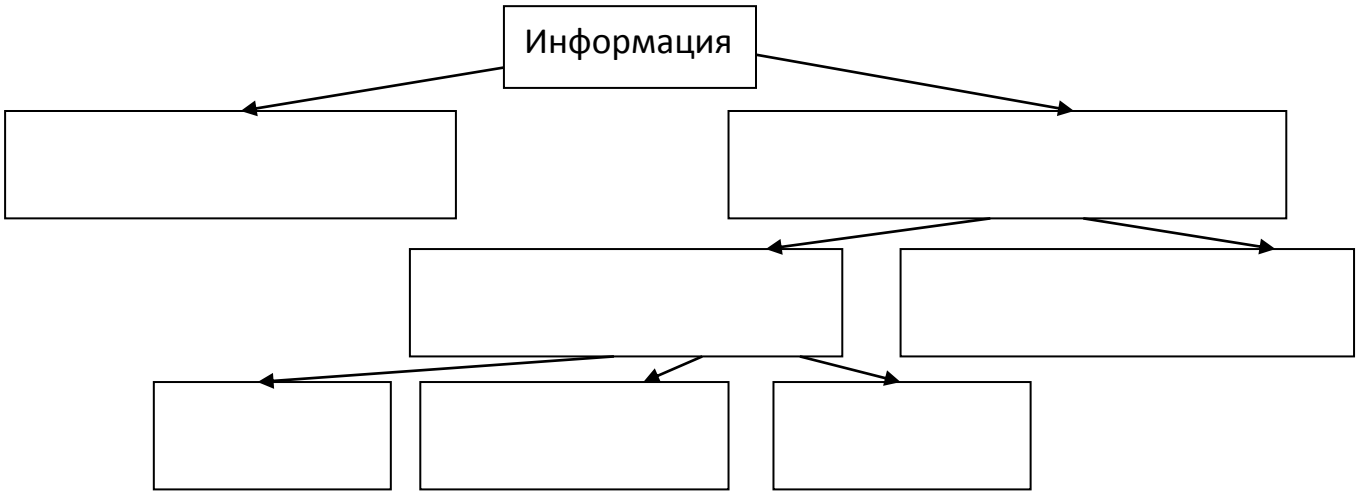
_____

_____

4.Составьте классификационную схему объектов защиты.



5. Классификация защищаемой информации по категориям доступа.



6. Все действующие АС, обрабатывающие конфиденциальную информацию, классифицируются в соответствии _____

_____

_____

_____

7. Классификация АС включает следующие этапы:

_____

_____

_____

_____

8. Исходными данными для классификации АС являются:

_____

_____

_____

_____

_____

_____

9. Определяющими признаками классификации АС являются:

_____

_____

_____

_____

10. 9 классов защищённости АС от НСД к информации, характеризуется определённой минимальной совокупностью требований по защите, и разделяются на 3 группы:

III группа – классы _____

_____

_____

_____

_____

II группа – классы _____

_____

_____

_____

_____

_____

I группа – классы _____

_____

_____

_____

_____

11. Подсистемы для обеспечения защиты от НСД:

_____

_____

_____

_____

12. **СВТ** – _____

_____

_____

СВТ классифицируются в соответствии с _____

_____

_____

14. Группы 7 классов защищённости СВТ от НСД

_____

_____

_____

_____

_____

15. В общем случае требования предъявляются к следующим показателям защищённости:

_____

_____

_____

_____

_____

16. ***Дискреционный принцип разграничения доступа*** предполагает ____

_____

_____

_____

17. ***Мандатный принцип разграничения доступа*** (*англ. Mandatory access control или MAC)*_____

_____

_____

_____

Задание 2. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС, выполнив задания, сохраните их в электронном документе под именем *Объекты защиты*.

1. Перечислите требования для АС по выделенным подсистемам в виде таблицы**.**

2. Отразите требования в зависимости от класса защищенности СВТ в виде таблицы.

Контрольные вопросы

1. Что понимают 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?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
4. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 7
Угрозы несанкционированного доступа к информации. Основные классы атак в сетях на базе TCP/IP

Цель: проанализировать основные угрозы несанкционированного доступа к информации, основные классы атак в сетях на базе TCP/IP**;** классифицировать основные виды угроз реализуемых по сети.

Задание 1. Ответьте на предложенные ниже вопросы или продолжите высказывание, используя Интернет-ресурс www.intuit.ru и СПС.

1. *ГОСТ* ***Р50922-2006*** *Защита информации. Основные термины и определения.* Настоящий стандарт устанавливает _____

_____

_____

В соответствии с ГОСТ ***Р50922-2006*** *защита информации от несанкционированного доступа* – это _____

_____

_____

_____

_____

3. В руководящих документах ФСТЭК ***несанкционированный доступ*** **(НСД)** – это _____

_____

_____

_____

4. Основные угрозы НСД:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

5. Комплекс программно – технических средств и организационных мер по ЗИ от НСД, условно состоит *из следующих четырех подсистем*:

_____

_____

_____

_____

6. Источником угрозы НСД может быть:

_____

_____

_____

7. При разработке модели нарушителя определяются следующие предположения:

_____

_____

_____

_____

_____

_____

8. Внешними нарушителями по отношению к АС являются:

_____

_____

_____

_____

_____

9. Внутренними нарушителями по отношению к АС являются:

_____

_____

_____

_____

10. Содержательная модель нарушителей отражает _____

_____

_____

_____

_____

11. Наиболее распространенные атаки в сетях на основе стека протоколов TCP/IP:

_____

_____

_____

_____

_____

_____

Задание 2. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС, выполнив задания, сохраните их в электронном документе под именем *Угрозы НСД*.

1. Отразите классификацию нарушителей по различным признакам в виде таблицы.

2. Математическая модель воздействия нарушителей представляет собой ...

3. Дайте характеристику наиболее опасных уязвимостей в виде таблицы.

4. Охарактеризуйте способы ослабления и контрмеры для каждого вида атак в сетях на основе стека протоколов TCP/IP в виде таблицы.

Контрольные вопросы

1. Назовите ГОСТ устанавливающий основные требования и определения в области защиты информации.
2. Дайте классификацию основных угроз НСД.
3. Перечислите, что включается в модель нарушителя ИБ. Их виды.
4. Перечислите виды угроз реализуемых по сети.

5. Перечислите наиболее распространенные атаки в сетях, способы их ослабления и контрмеры.

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
4. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 8
Программно-математическое воздействие

Цель: изучить основные виды программно-математического воздействия на информацию, методы обнаружения вирусов.

Задание. Ответьте на предложенные ниже вопросы или продолжите фразы, используя Интернет-ресурс **www.intuit.ru**, поисковые системы. Ответы должны быть полные в соответствии с поставленным вопросом.

1. **Программно-математическое воздействие** – это _____

_____

_____

Вредоносная программа – _____

_____

_____

_____

2. Основными путями проникновения вредоносных программ в АС, в частности, на компьютер, являются:

_____

_____

3. Основными видами вредоносных программ являются:

_____

_____

_____

_____

4. К программным закладкам относятся _____

_____

_____

5. Программные закладки в зависимости от метода их внедрения в систему делятся:

_____

_____

_____

_____

_____

_____

6. Вирус (компьютерный, программный) – _____

_____

_____

_____

Обязательным свойством программного вируса является _____

_____

_____

_____

_____

7. ***Червь*** – _____

_____

_____

_____

8. Сигнатурный метод основан _____

_____

_____

Сигнатура – это _____

_____

_____

Эвристический метод представляет собой _____

_____

_____

9. Эвристические методы:

_____

_____

_____

_____

_____

_____

_____

_____

10. В составе антивируса обязательно должны присутствовать следующие модули (охарактеризуйте их):

_____

_____

_____

_____

_____

_____

_____

_____

_____

Контрольные вопросы

1. Что представляет собой программно-математическое воздействие на информацию.
2. Назовите основные пути проникновения вредоносных программ в АС.
3. Перечислите основные виды вредоносных программ.
4. Перечислите виды программных закладок.

5. В чем суть сигнатурного и эвристического методов?

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.
2. Справочно-правовая система Гарант.
3. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 9
Классификация технических каналов утечки информации. Информационный сигнал и его характеристики

Цель: проанализировать технические каналы утечки информации; физическую суть возникновения различных каналов утечки.

Задание 1. Ответьте на предложенные ниже вопросы или продолжите высказывания, используя Интернет-ресурс www.intuit.ru и СПС.

1. ***Утечка*** – это _____

_____

_____

Утечка по техническому каналу – это _____

_____

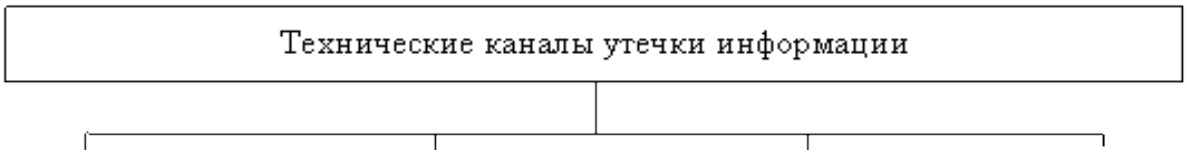
_____

_____

_____

2. Изобразите схематически структуру технического канала утечки информации.

3. Классификация технических каналов утечки информации (схема)



4. Утечка информации в материально-вещественном канале происходит ___

_____

_____

_____

_____

5. Угрозы, возникающие в результате реализации технических каналов утечки информации:

_____

_____

_____

_____

6. Физический процесс, параметры которого способны изменяться в зависимости от передаваемой информации называется _____

_____

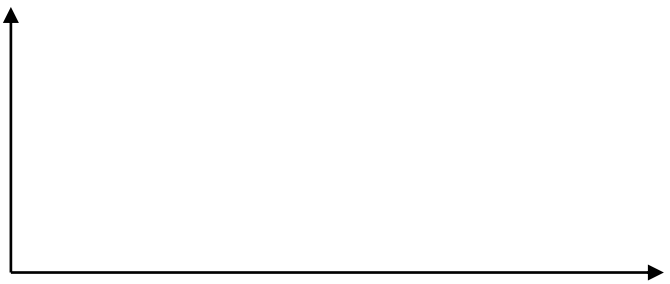
Этот процесс изменения параметров носителя называют _____

7. При регистрации сигнала основной задачей является _____

_____

_____

8. Изобразите аналоговый и цифровой сигналы.

Аналоговый сигнал	
Цифровой сигнал	

9. Признак защищаемого сигнала, позволяющий обнаруживать и распознавать его среди других сигналов, называется _____

10. Параметры аналоговых сигналов:

_____ _____

_____ _____

_____ _____

_____ _____

11. Параметры дискретных (цифровых) сигналов:

_____ _____

_____ _____

_____ _____

_____ _____

12. ***Амплитудная модуляция*** — _____

_____

Частотная модуляция – _____

_____

Фазовая модуляция — _____

_____

13. Отразите графически процессы модуляции аналогового сигнала цифровыми данными.

Контрольные вопросы

1. Дайте классификацию технических каналов утечки информации.
2. Перечислите угрозы, возникающие в результате реализации технических каналов утечки информации.
3. Перечислите параметры аналоговых и цифровых сигналов.
4. Дайте определение амплитудной, частотной и фазовой модуляций.

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/

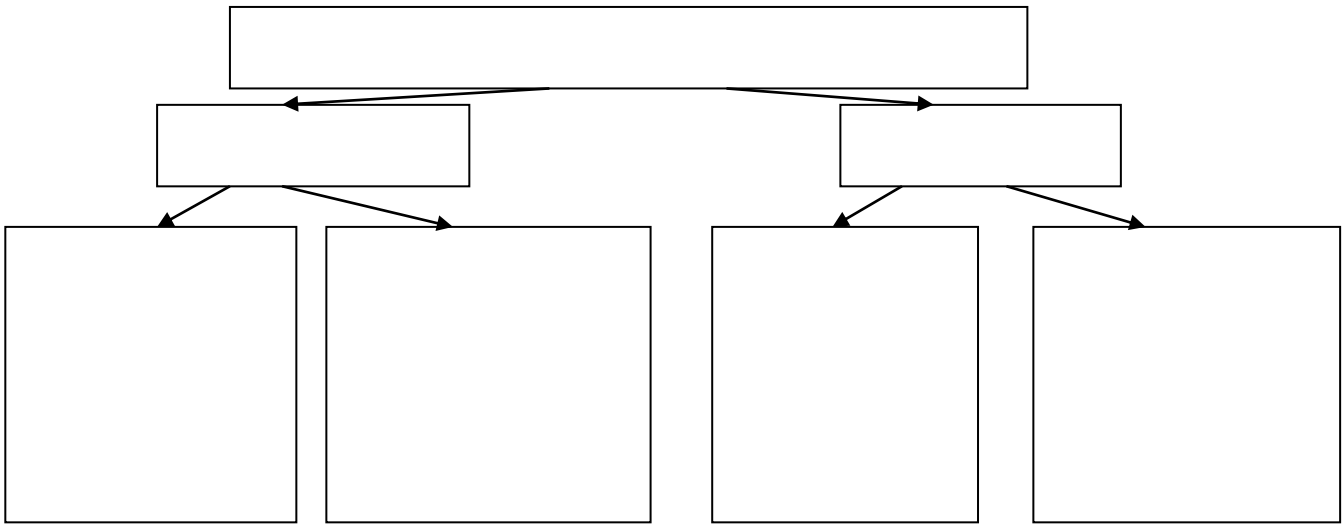
4. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 10
Защита акустической (речевой) информации

Цель: проанализировать способы защиты акустической (речевой) информации.

Задание. Ответьте на предложенные ниже вопросы, используя Интернет-ресурс www.intuit.ru и СПС.

1. Методы защиты акустической информации и их содержание.



2. Цель применения пассивных средств защиты информации_____

_____

_____

_____

3. Цель звукоизоляции: _____

_____

_____

_____

4. Для уменьшения утечки акустической информации через **окна** _____

_____

_____

_____

_____

_____

Для уменьшения утечки акустической информации через **двери** _____

_____

_____

_____

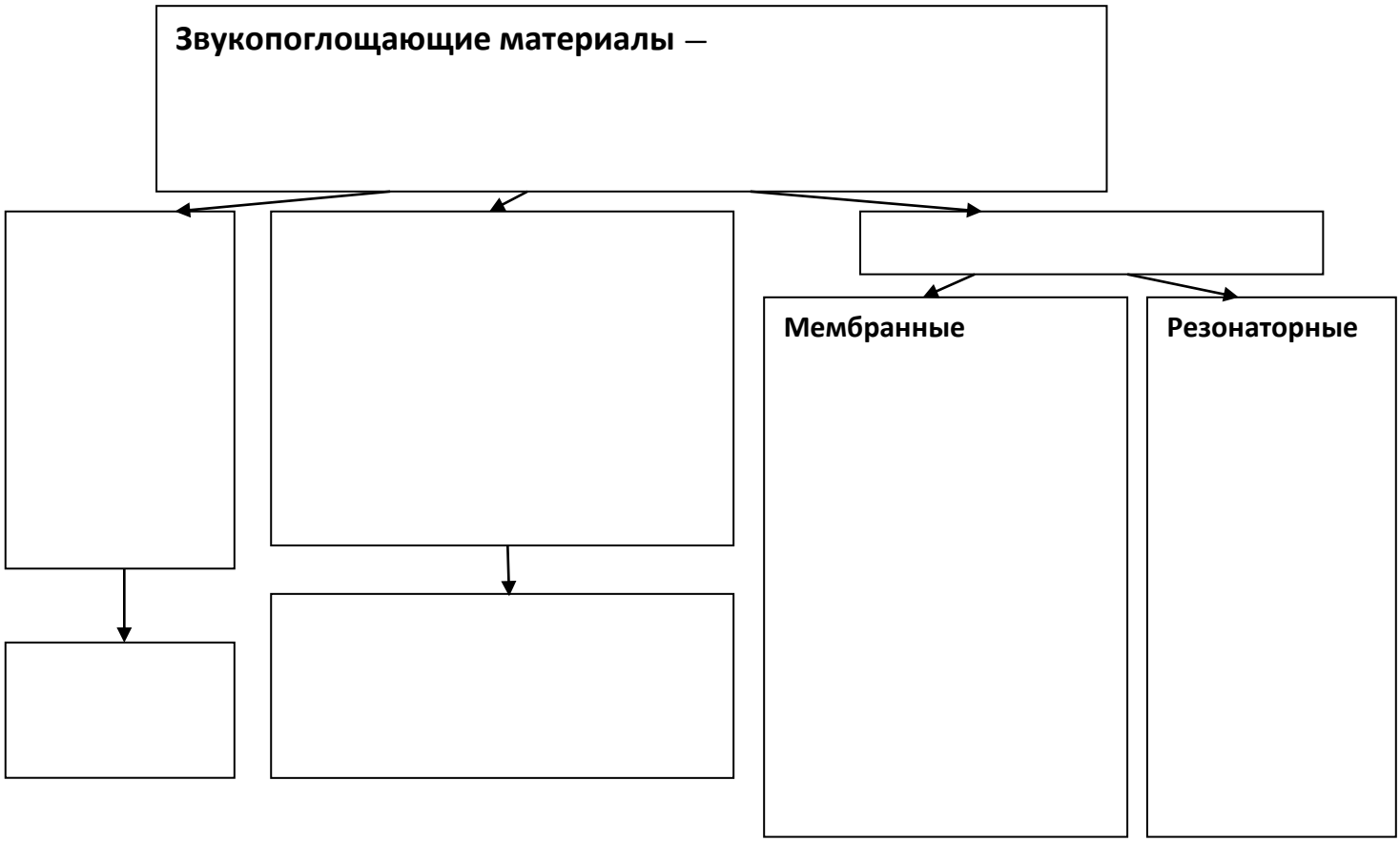
_____

_____

_____

5. Составьте классификационную схему звукопоглощающих материалов.

Методические рекомендации. Схема должна содержать три уровня. Верхний уровень (определение) → виды (со способом поглощения) → примеры.



7. В качестве активного способа защиты акустической информации используют _____

8. Виды помех (с характеристиками) использующиеся для зашумления:

_____

_____

_____

_____

_____

_____

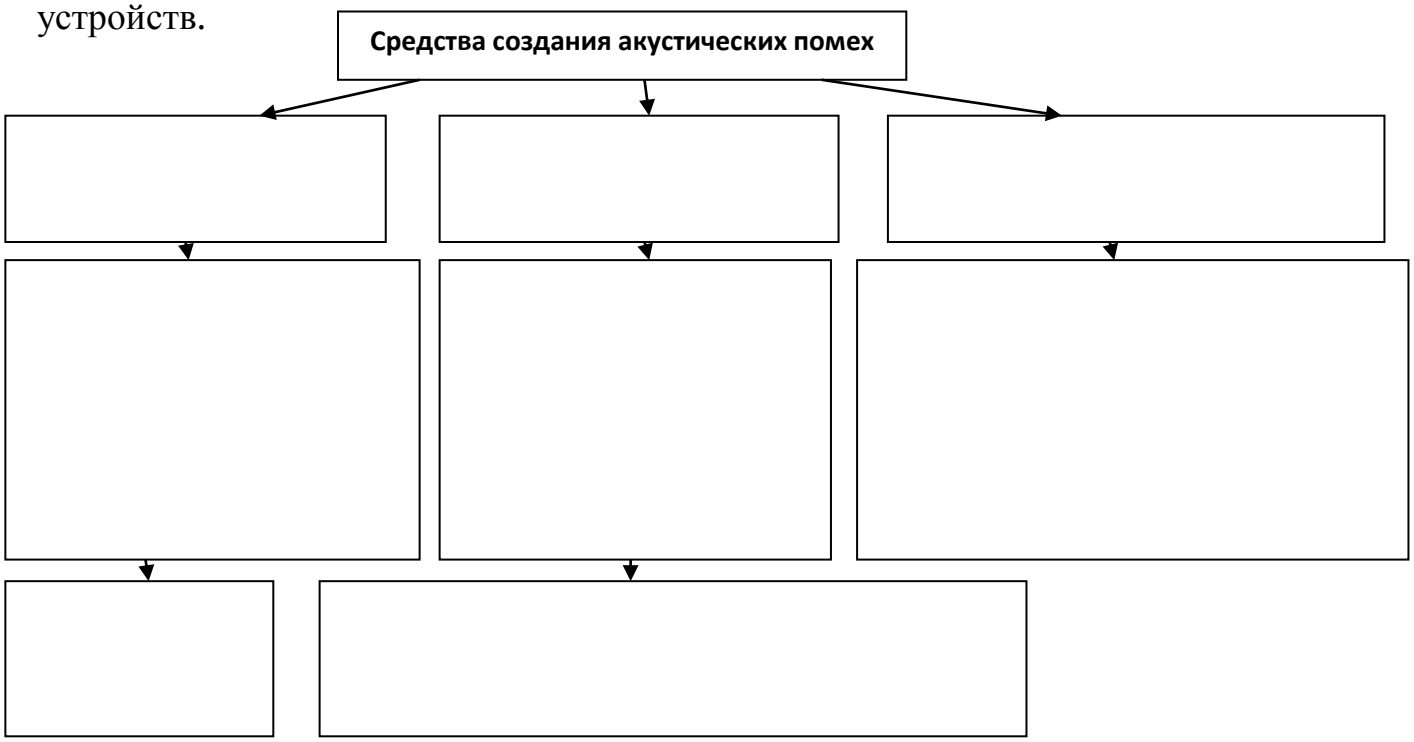
_____

_____

_____

_____

9. Классификационная схема средств создания акустических помех с указанием принципа защиты каждого средства и конкретными примерами устройств.



10. Средства защиты, использующиеся для подавления диктофонов_____

_____

Принцип подавления_____

_____

_____

_____

Примеры таких устройств_____

_____

_____

_____

11. Защищаемые помещения должны размещаться в пределах контролируемой зоны (КЗ) с учетом следующих рекомендаций (в соответствии с СТР-К):

_____

_____

_____

_____

Контрольные вопросы

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).

Список используемых источников

1. Справочно-правовая система КонсультантПлюс.

2. Справочно-правовая система Гарант.

3. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/

4. Интуит. Электронный ресурс: заглавие с экрана. Режим доступа: www.intuit.ru.

Практическое занятие 11

Средства акустической разведки

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

Задание. 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 перед группой 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.

Задание выполняется индивидуально или в парах, анализируемое средство акустической разведки распределяется преподавателем.

Средства акустической 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.

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
2. Бюро Научно-Технической Информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.bnti.ru.
3. Спецтехника и связь. Электронный ресурс: заглавие с экрана. Режим доступа: www.st-s.su

4. АФА. Агентство технической защиты информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.afa.biz.ua

Практическое занятие 12

Средства радио- и радиотехнической разведки

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

Задание. 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 перед группой 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.

Задание выполняется индивидуально или в группах, анализируемое средство акустической разведки распределяется преподавателем.

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.

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/
2. Бюро Научно-Технической Информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.bnti.ru.
3. АФА. Агентство технической защиты информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.afa.biz.ua

Практическое занятие 13
Системы защиты территории и помещений

Цель: проанализировать виды охранных систем, их принципы работы, назначение, параметры и особенности применения, техническое исполнение.

Задание. Проанализируйте системы защиты территории и помещений. Составьте обзор рынка современных систем защиты территории и помещений. Оформите отчет в виде текстового файла и презентации к сообщению (будьте готовы к выступлению перед группой с этим отчетом).

Методические рекомендации

В отчете обратите внимание на отражение следующих вопросов:

- принцип работы;
- назначение;
- устройство;
- особенности и возможности;
- основные характеристики;
- техническая реализация отечественных и зарубежных производителей.

Задание выполняется индивидуально или в группах, анализируемое средство акустической разведки распределяется преподавателем.

Системы защиты территории и помещений для анализа

1. Инфракрасные системы.
2. Системы защиты ИК-датчиков.
3. Оптоволоконные системы.
4. Емкостные системы охраны периметров.
5. Вибрационные системы и вибрационно-сейсмические системы
6. Радиолучевые системы.
7. Системы «активной» охраны периметров.

Список используемых источников

1. Технические средства и методы защиты информации. Учебное пособие для вузов/А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др., под редакцией А.П. Зайцева и А.А. Шелупанова. – 4-е изд., испр. И доп. – М.: Горячая линия–Телеком, 2012. – 616 с.
2. Торокин А.А. Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2009.

Практическое занятие 14

Системы охранной, тревожной и пожарной сигнализации

Цель: изучить системы охранной, тревожной и пожарной сигнализации, их принципы работы, назначение, параметры и особенности применения, техническое исполнение.

Методические рекомендации

Используя дополнительные источники предложенные преподавателем, отчет необходимо оформить в тетради и электронном документе *Системы СОТС и СПС*.

Задание 1. Проанализируйте системы охранной, тревожной и пожарной сигнализации, их принципы работы, назначение, параметры и особенности применения.

1. Системы СОТС (система охранной и тревожной сигнализации) и СПС (система пожарной сигнализации) предназначены _____

_____

_____

2. СОТС содержит следующие основные элементы:

_____

_____

_____

_____

_____

_____

_____

_____

СПС содержит следующие основные элементы:

_____

_____

_____

_____

_____

_____

_____

3. Основной задачей охранно-пожарной сигнализации (ОПС) является ____

_____

_____

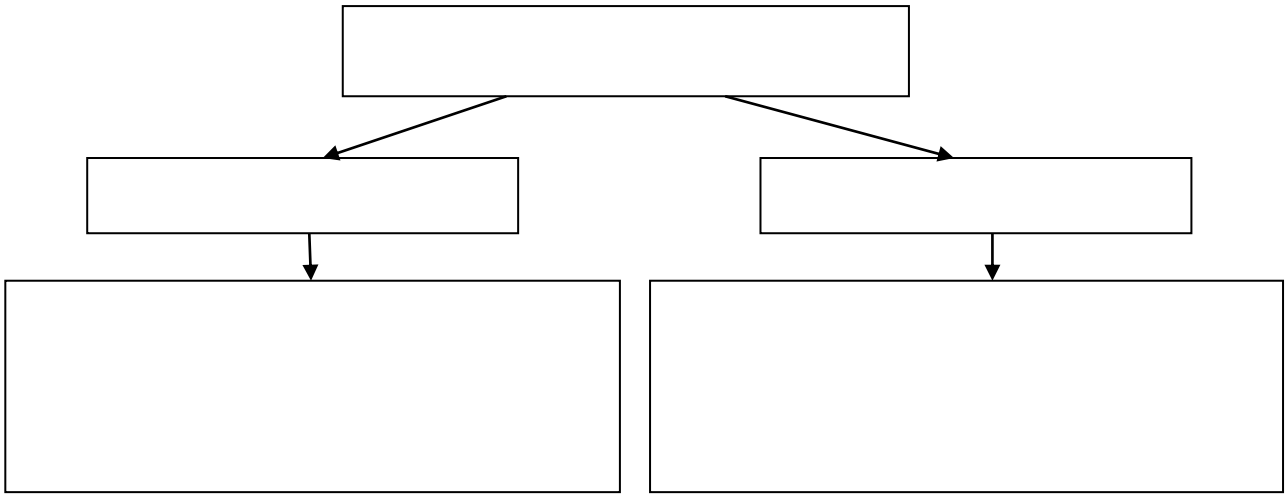
_____

4. Технические средства обнаружения (ТСО) – _____

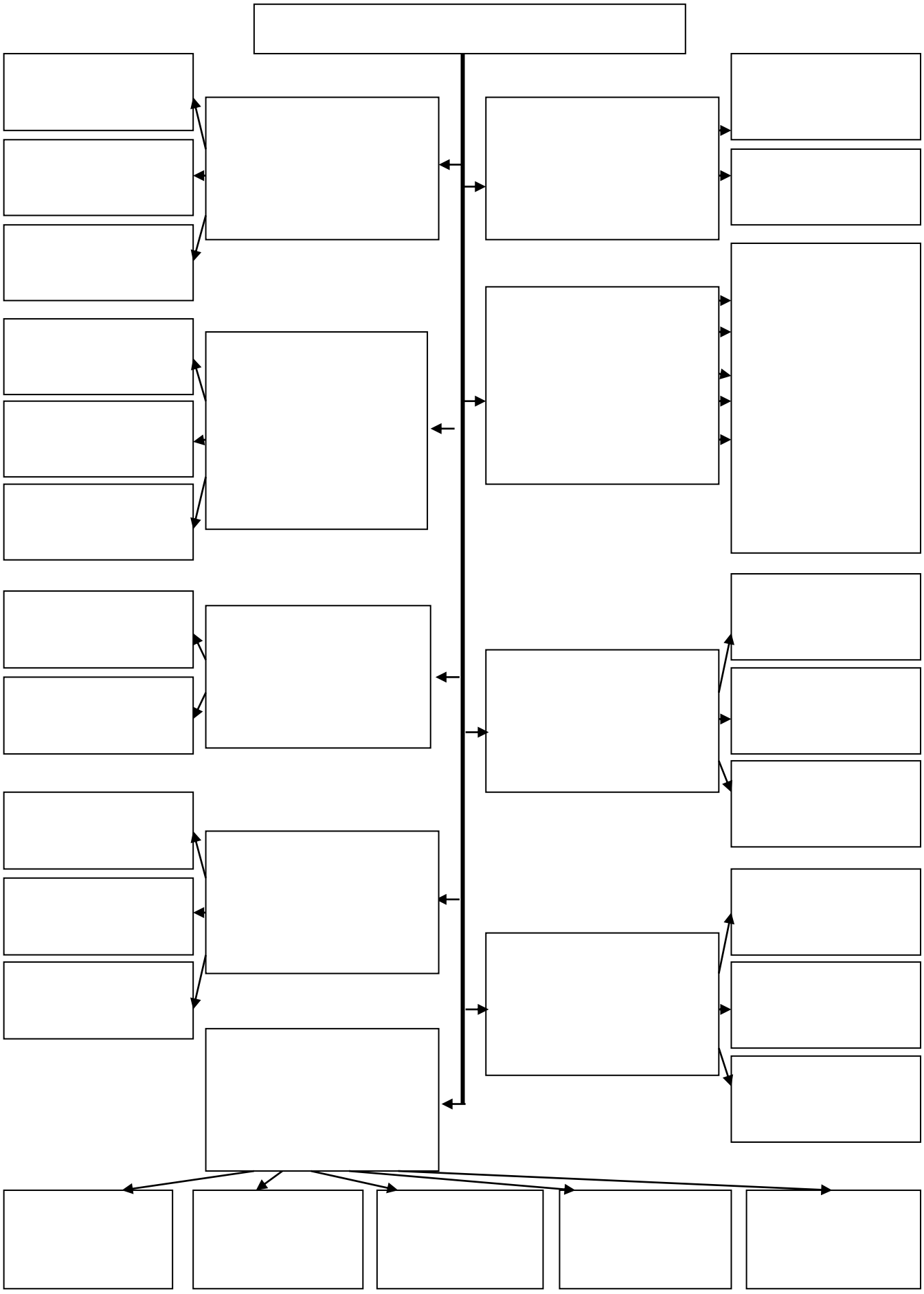
_____

_____

5. Схема деления извещателей ОПС по принципу формирования информационного сигнала о проникновении на объект или пожаре.



6. Классификация извещателей охранных (ИО) по признакам функционального назначения.



7. По виду контролируемого признака пожара автоматические извещатели пожарные **(**ИП) подразделяют**:**

_____

_____

_____

_____

_____

_____

_____

8. Функциональные особенности некоторых применяемых на практике охранных извещателей**.**

Вид извещателя	**Принцип действия**	**Область применения**

9. Извещатели тревожной сигнализации предназначены _____

_____

_____

_____

_____

10. **Извещатель пожарный** – _____

_____

_____

11. Функциональные особенности некоторых применяемых на практике пожарных извещателей.

Вид извещателя	**Принцип действия**	**Область применения**

Вид извещателя	Принцип действия	Область применения

12. **Прибор приемно-контрольный (ППК) охранный (охранно-пожарный)** – _____

_____

_____

_____

_____

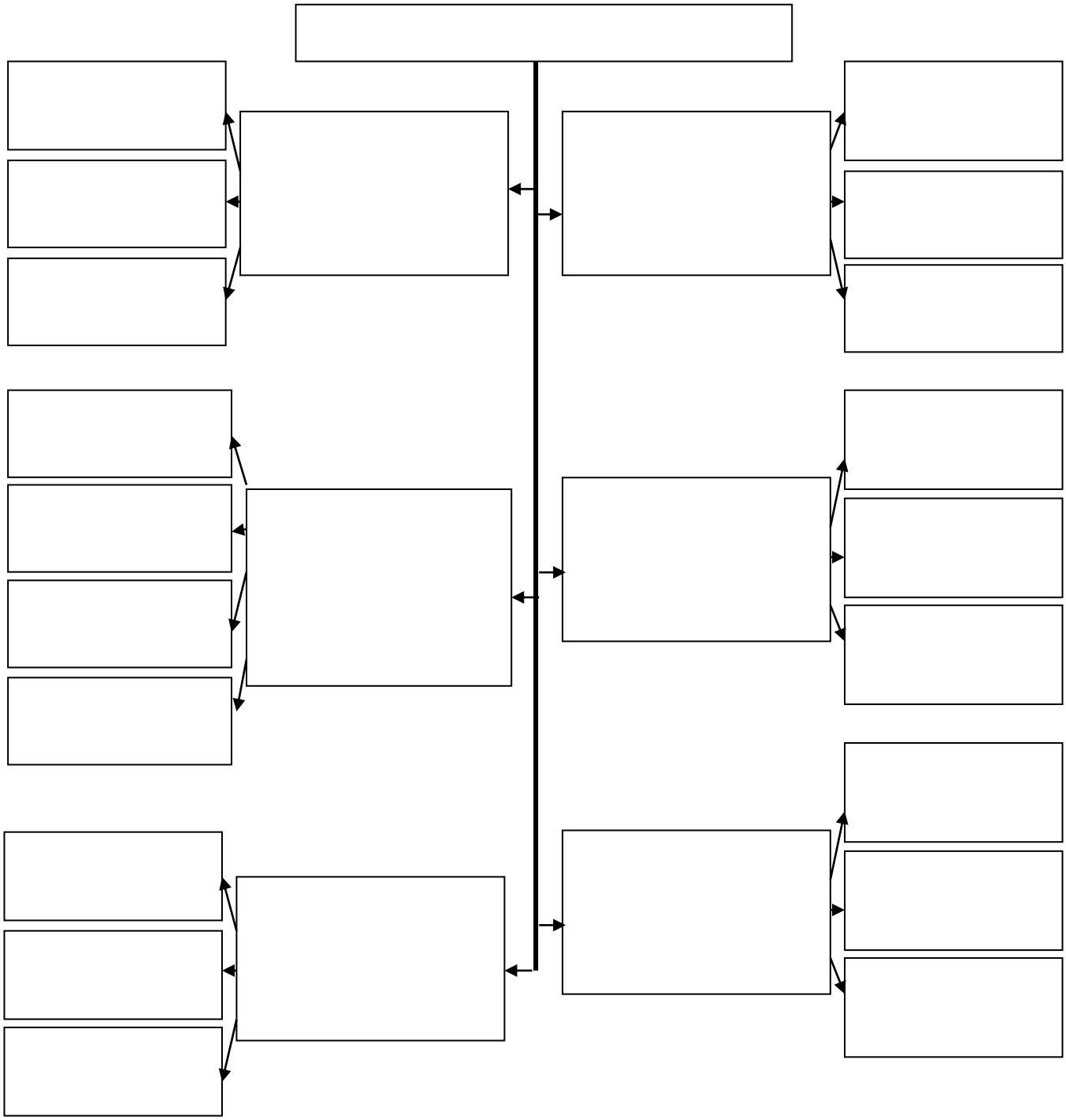
_____

_____

_____

_____

13. Классификация охранных ППК.



14. ППК для локальной сигнализации должны дополнительно к основным функциям обеспечивать:

_____

_____

_____

_____

_____

15. Основными параметрами ППК охранного являются **информационная емкость и информативность**.

Емкость информационная – это _____

_____

_____

_____

_____

_____

Информативность – это _____

_____

_____

16. Информативность для автономных ППК (виды извещений):

_____

_____

_____

_____

_____

_____

_____

_____

17. **ППК пожарный** – _____

_____

_____

_____

_____

_____

18. Система оповещения (СО) на охраняемом объекте и его территории создается для _____

_____

_____

_____

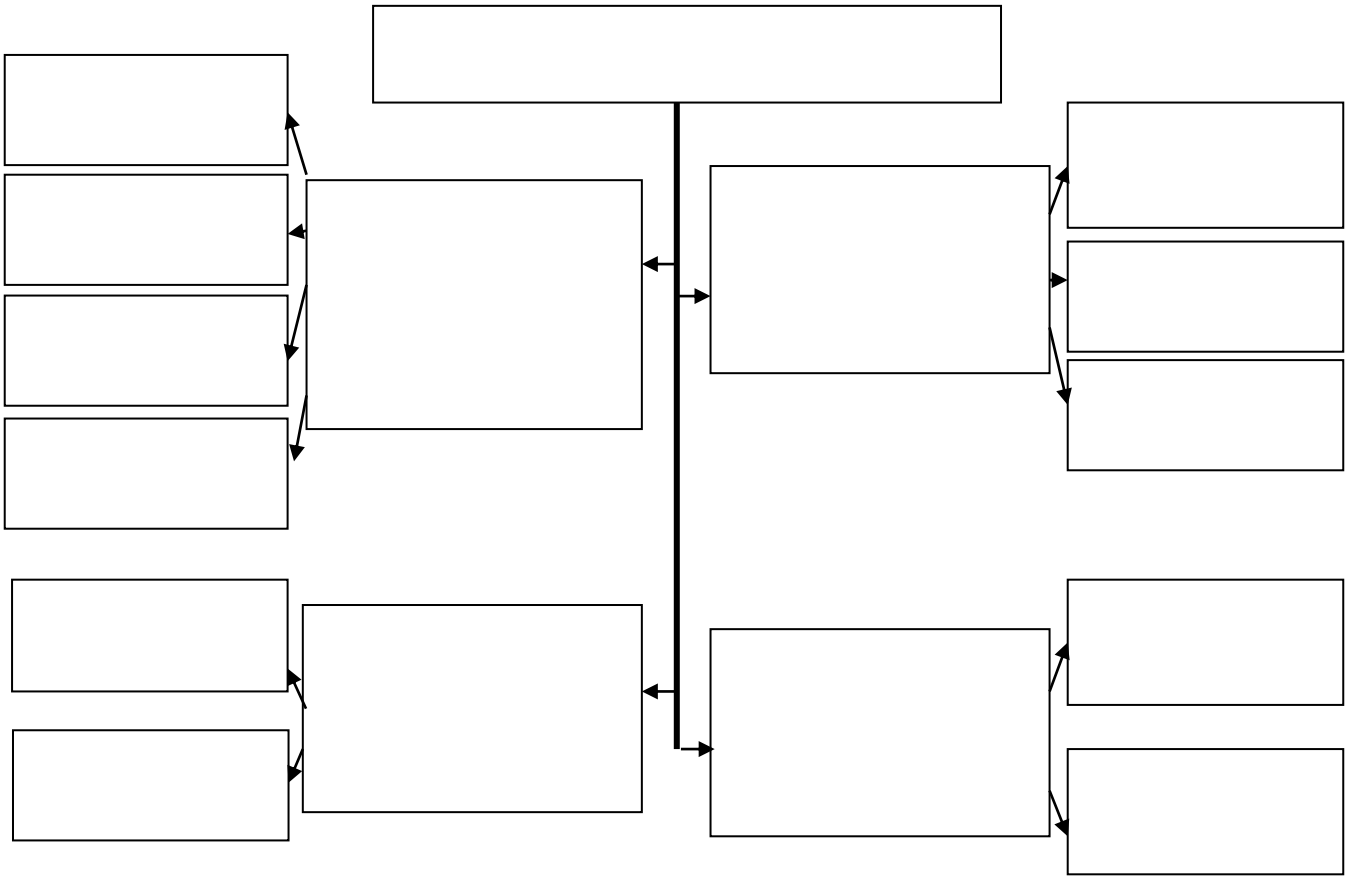
Оповещатель для СБ _____

_____

_____

_____

19. Классификация СО



20. **Системы передачи извещений (СПИ) о проникновении и пожаре** представляет собой _____

_____

_____

_____

_____

21. По типу используемых линий (каналов) связи системы передачи извещений делятся на системы, использующие:

_____

_____

_____

_____

_____

_____

_____

_____

Задание 2. Приведите конкретные примеры каждого типа устройств с указанием характеристик (в виде таблицы) и изображением внешнего вида, соблюдая в электронном документе правила оформления таблиц и иллюстраций. Информацию сохраните в электронный документ под именем *Системы СОТС и СПС*.

Контрольные вопросы

1. Назовите основные элементы СОТС и СПС Для чего они предназначены?
2. Опишите признаки, по которым классифицируются охранные и пожарные извещатели.
3. Перечислите виды ИО и ИП. Опишите принципы их функционирования.
4. Для чего предназначен ППК, каковы их виды?
5. Что такое информативность ППК?
6. Назовите виды систем оповещения.
7. Что представляют собой СПИ о проникновении и пожаре?

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/

2. Бюро Научно-Технической Информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.bnti.ru.

4. АФА. Агентство технической защиты информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.afa.biz.ua

5. Волхонский В.В. Устройства охранной сигнализации. Учебное пособие. – СПб: Университет ИТМО, 2015

Практическое занятие 15
Системы контроля и управления доступом

Цель: изучить системы контроля и управления доступом, их принципы работы, назначение, параметры и особенности применения, техническое исполнение.

Методические рекомендации

Используя дополнительные источники предложенные преподавателем, отчет необходимо оформить в тетради и электронном документе *Системы КУД.*

Задание 1. Проанализируйте системы контроля управления доступом, их принципы работы, назначение, параметры и особенности применения.

1. Основные понятия и определения

Контрольно-пропускной режим – _____

_____

_____

_____

_____

_____

Система контроля и управления доступом (СКУД) как на сам объект, так и в отдельные его помещения – _____

_____

_____

_____

Задачи СКУД в составе СБ:

_____

_____

_____

_____

_____

_____

_____

_____

_____

Идентификация предполагает _____

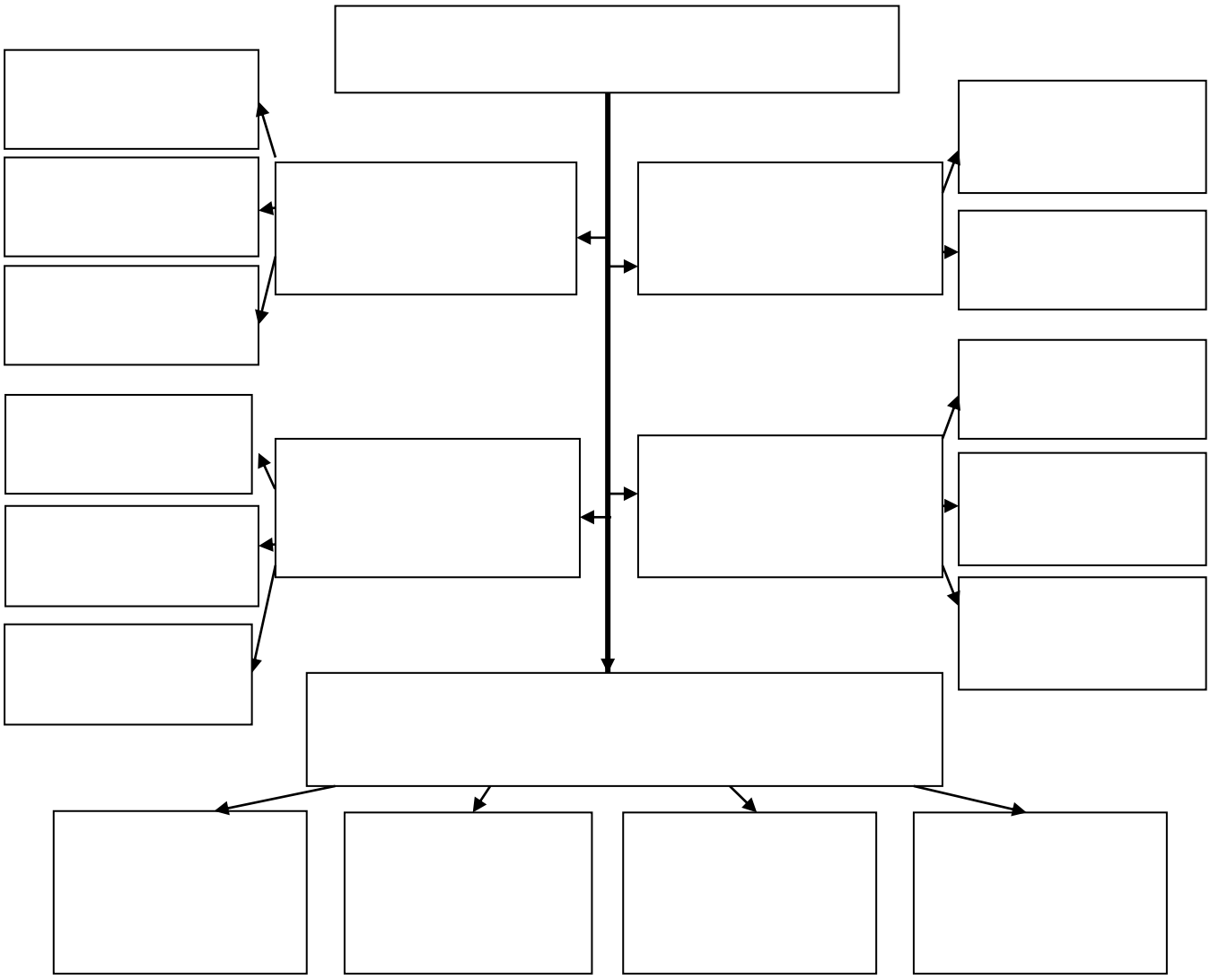
_____

_____

Аутентификация подразумевает _____

СКУД включает следующие программно-технические средства:

2. Классификация современных СКУД



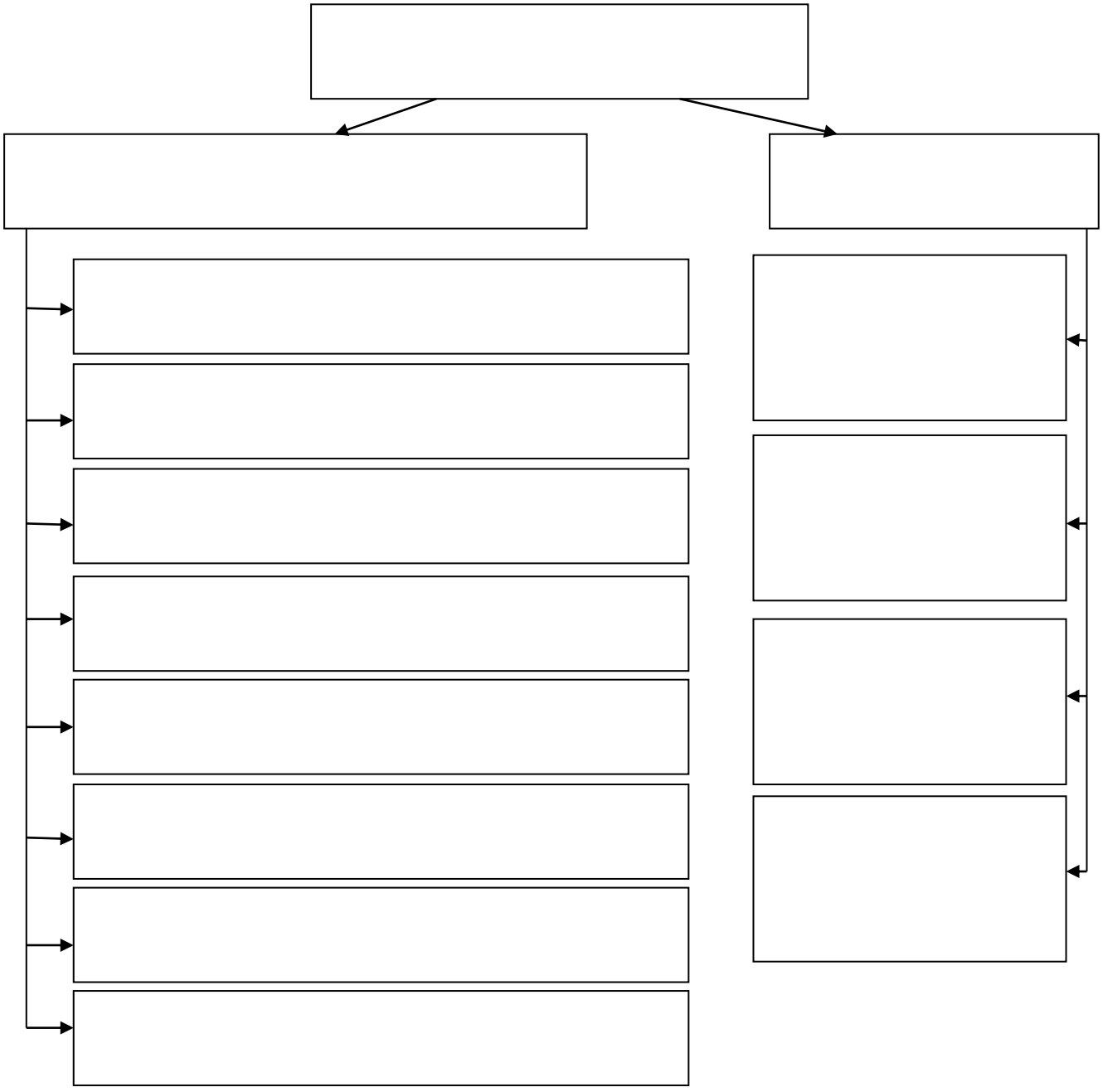
3. **Устройство идентификации доступа (идентификаторы и считыватели)** _____

_____

_____

_____

4. Классификация устройств идентификации доступа



5. **Идентификатор доступа –** _____

_____

_____

6. Атрибутные идентификаторы – _____

_____

7. Биометрические идентификаторы – _____

_____

8. Атрибутные идентификаторы, используемые при организации доступа.

Идентификатор	**Принцип действия**	**Достоинства**	**Недостатки**

9. **Биометрические технологии** предполагают _____

_____

_____

10. Этапы работы биометрических систем:

_____

_____

_____

_____

_____

_____

_____

_____

11. **При идентификации** в биометрических системах_____

_____

_____

_____

12. **При верификации** в биометрических системах _____

_____

_____

_____

_____

13. Для увеличения пропускной способности биометрических систем _____

_____

_____

_____

14. **Точки прохода СКУД – _____**

_____

_____

_____

15. **Считыватель** – _____

_____

_____

16. **Кодонаборные устройства СКУД – _____**

_____

_____

17. Кодонаборные терминалы предоставляют возможность пользователю, если он действует по принуждению _____

_____

_____

18. Задачи средств сбора, обработки, отображения информации и управления в составе СКУД:

_____

_____

_____

_____

_____

_____

Задание 2. Приведите конкретные примеры каждого типа устройств с указанием характеристик (в виде таблицы) и изображением внешнего вида, соблюдая в электронном документе правила оформления таблиц и иллюстраций. Информацию сохраните в электронный документ под именем *Системы КУД.*

Контрольные вопросы

1. Что такое контрольно-пропускной режим?
2. Что подразумевается под СКУД. Каковы ее задачи?

3. Дайте определения идентификации и аутентификации.

4. Назовите программно-технические средства СКУД.

5. Охарактеризуйте классификацию современных СКУД.

6. Дайте классификацию устройств идентификации доступа.

7. Что такое идентификатор доступа? Какие идентификаторы существуют?

8. Дайте характеристику атрибутных идентификаторов, используемых при организации доступа.

9. На чем основана биометрическая СКУД?

10. В чем отличие идентификации от верификации в биометрических СКУД?

11. Дайте характеристику кодонаборных устройств.

12. Перечислите задачи средств сбора, обработки, отображения информации и управления в составе СКУД.

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/

2. Бюро Научно-Технической Информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.bnti.ru.

3. АФА. Агентство технической защиты информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.afa.biz.ua

4. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. - М.: Горячая линия - Телеком, 2015. - 272 с.: ил.

Практическое занятие 16
Телевизионные системы безопасности

Цель: изучить телевизионные системы безопасности, их принципы работы, назначение, параметры и особенности применения, техническое исполнение.

Методические рекомендации

Используя дополнительные источники предложенные преподавателем, отчет необходимо оформить в тетради и электронном документе *Системы ОТ*.

Задание 1. Проанализируйте системы охранного телевидения, их принципы работы, назначение, параметры и особенности применения.

1. Цель телевизионной системы охранного телевидения _____

_____

_____

_____

_____

2. ***Система охранная телевизионная*** **(СОТ) – _____**

_____

_____

_____

3. Функции системы охранного телевидения:

_____

_____

_____

_____

_____

_____

4. Виды просмотра видеоинформации:

_____

_____

_____

_____

_____

_____

_____

_____

_____

5. Обобщенная структурная схема СОТ.

6. **Видеокамера** представляет собой _____

_____

_____

_____

7. В зависимости от конструктивного исполнения, технических характеристик и условий эксплуатации видеокамеры подразделяют:

_____

_____

_____

_____

_____

_____

8. Параметры видеокамер.

Оптический формат – _____

_____

Разрешающая способность видеокамеры (разрешение) **–** _____

_____

_____

Рабочий диапазон освещенностей – _____

_____

_____

Пороговая чувствительность (чувствительность) – _____

_____

_____

_____

9. Виды объективов видеокамер

Вид объектива	Область применения. Особенности

10. Цели системы охранного телевидения в соответствии с требованиями к качеству.

Цель СОТ	Пояснения цели	Требования к качеству изображения

11. Технические решения, направленные на улучшение характеристик видеокамер.

Видеокамера или режим работы	Техническое решение

12. **Поворотная видеокамера** – _____
_____
_____
_____

13. «Автослежение» – _____
_____
_____
_____
_____

14. Видеозапись в составе СОТ может быть реализована на базе устройств видеозаписи – _____
_____
_____
_____
_____

Устройства видеозаписи в составе должны обеспечивать запись и хранение видеоинформации в следующих режимах:

При воспроизведении записи видеорегистратор позволяет:

15. Варианты системы управления видеонаблюдением:

16. Основные параметры видеорегистраторов и их характеристика:

Для того чтобы уменьшить большие объемы видеозаписей, используют

17.***Видеодетекторы движения*** позволяют _____

18. Применение ***видеоанализа*** при решении различных задач охраны и контроля объектов видеонаблюдения:

19. **Определение несанкционированного прохода** средствами видеоанализа позволяет _____

_____

_____

20. **Обнаружение пересечения границы** позволяет _____

_____

_____

_____

_____

21. Сетевые функции ЦВР подразумевают реализацию следующих возможностей:

_____

_____

_____

_____

_____

22. Для установки видеокамеры в неблагоприятных условиях применяются _____

_____

_____

_____

Кожухи для видеокамер можно разделить:

_____

_____

_____

_____

_____

_____

Класс защиты кожуха от воздействий пыли и воды *(IP - International Protection)* обозначается _____

_____

_____

23. Поддержание работоспособности видеокамеры в условиях низких температур достигается _____

24. **Цифровая СОТ – _____**

_____

_____

_____

IP – камера – _____

_____

_____

25. Достоинства и недостатки сетевых видеокамер.

Достоинства	**Недостатки**

Задание 2. Приведите конкретные примеры каждого типа рассмотренных выше устройств с указанием характеристик (в виде таблицы) и иллюстрацией внешнего вида, соблюдая в электронном документе правила оформления таблиц и иллюстраций. Информацию сохраните в электронный документ под именем *Системы ОТ.*

Контрольные вопросы

1. Что такое система охранного телевидения? Цель ее создания?
2. Каковы функции СОТ?
3. Назовите виды просмотра видеоизображений.
4. Перечислите виды видеокамер и их параметры.
5. Охарактеризуйте объективы и область их применения в СОТ.
6. Перечислите требования к качеству изображений.
7. Назовите режимы хранения видеозаписей.
8. Перечислите варианты систем управления видеонаблюдением.
9. Дайте характеристику параметров видеорегистратора.
10. Охарактеризуйте функции видеодетектирования и видеоанализа.
11. Перечислите сетевые функции ЦВР.
12. Охарактеризуйте цифровые СОТ.
13. Перечислите достоинства и недостатки сетевых видеокамер.

Список используемых источников

1. Сайт Федеральной службы по техническому и экспортному контролю. Электронный ресурс: заглавие с экрана. Режим доступа: http://www.fstec.ru/

2. Бюро Научно-Технической Информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.bnti.ru.

3. АФА. Агентство технической защиты информации. Электронный ресурс: заглавие с экрана. Режим доступа: www.afa.biz.ua

4. Волковицкий В.Д., Волхонский В.В. Цифровые системы ТВ-наблюдения // БДИ. Безопасность, достоверность, информация. СПб., 2015. № 5. С. 38-47.

5. Гедзберг Ю.М. Охранное телевидение. - М.: Горячая линия - Телеком, 2014. - 312 с.: ил.

Практическое занятие 17

Моделирование технической разведки по исходным данным для объекта информатизации

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

Методические рекомендации

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.

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.

Схема объекта представлена на рисунке 17.1.

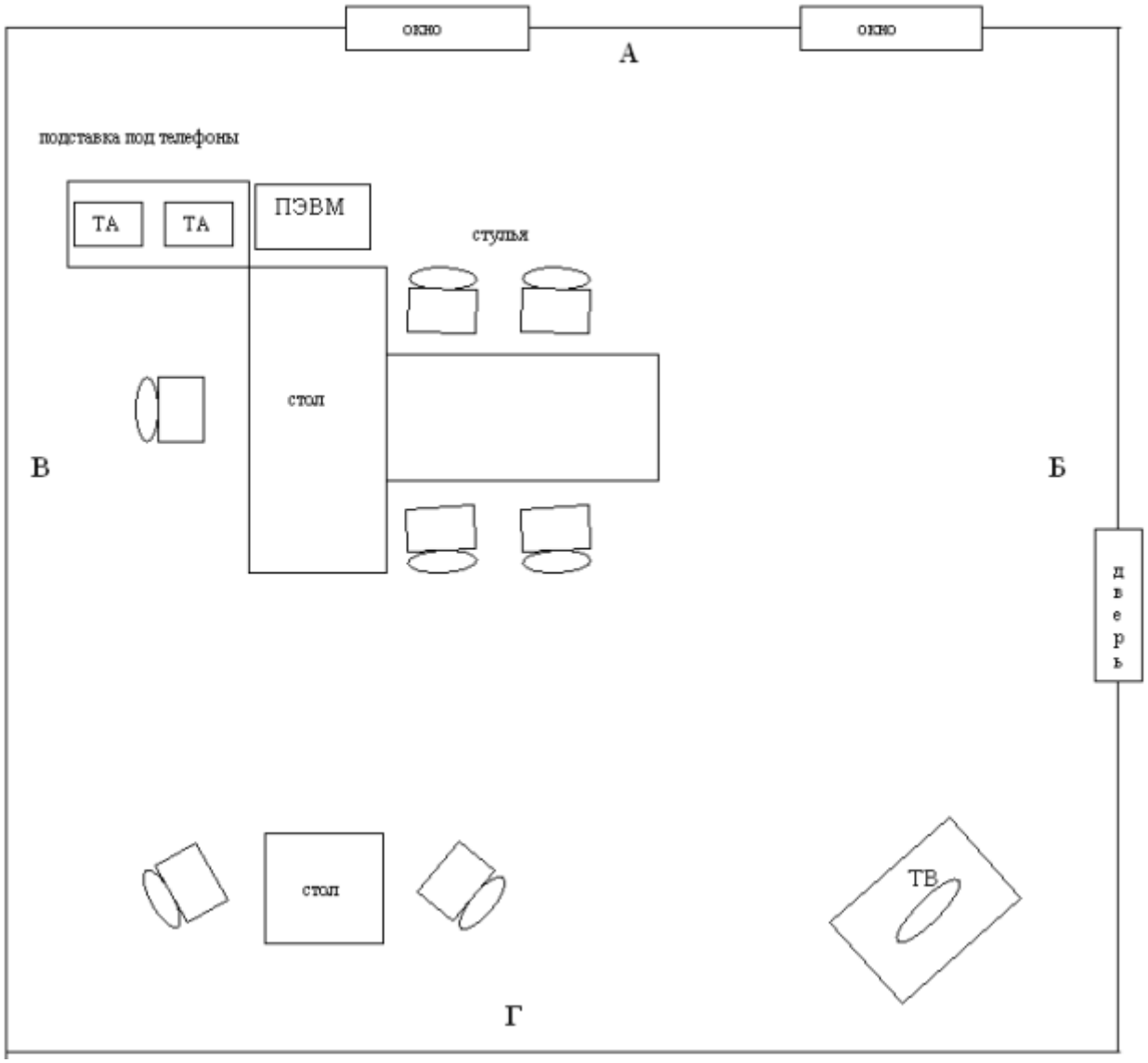


Рисунок 17.1 – Схема объекта

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.

Задание. Продолжите анализ защищенности объекта, по следующим направлениям:

– 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....».

Практическое занятие 18

Моделирование инженерно-технической системы защиты информации по исходным данным для объекта информатизации

Задание. Выявите и проанализируйте возможные угрозы информационной безопасности объекта, оценив вероятность их осуществления. Предложите способы уменьшения реализации выделенных угроз техническими методами защиты информации. Аргументируйте выбор технических средств ЗИ, начертите планы территории и поэтажные планы помещений с изображением на них выбранных ТСЗИ. Оформите отчет.

Методические рекомендации

При моделировании системы защиты информации (**ее технической составляющей**) необходимо предусмотреть расположение систем контроля

управления доступом (СКУД), системы видеонаблюдения, системы охранной сигнализации на объекте, инженерно-технические защитные сооружения и т.д.

В отчете (электронный документ) необходимо:

- расширить описание защищаемого объекта;
- перечислить возможные угрозы ИБ;
- изобразить планы территории и помещений;
- предложить планы размещения систем КУД, видеонаблюдения, охранно-пожарной сигнализации;
- выбрать и описать (характеристики дать в виде таблицы) конкретные устройства каждой системы;
- каждый элемент предложенной вами системы защиты информации должен быть аргументирован (вероятность реализации, какой из угроз ИБ уменьшает данный элемент ЗИ).

Описание объекта 1. Объект защиты расположен в жилом доме и занимает два этажа. Здание окружено другими жилыми домами. Стены объекта выполнены из кирпичной кладки, толщина кладки 2 кирпича. На объекте защиты установлены окна с двойным остеклением. Двери, находящиеся на объекте защиты являются металлическими. Вход на объект расположен в центральной части здания. Охрана объекта осуществляется круглосуточно собственной службой безопасности. Устройства управления механизмами открывания прохода, охранным освещением размещены в помещении проходной объекта защиты. Возможность доступа к устройствам управления посторонних лиц исключается. Освещение объекта электрическое. Электропроводка по стенам проложена в металлических и пластиковых кабель-каналах, за подвесными потолками в пластиковых трубах. Система гарантированного электропитания на объекте отсутствует.

В здании смонтированы и находятся в рабочем состоянии следующие инженерные системы: отопления; холодного и горячего водоснабжения; вентиляции и кондиционирования воздуха; автоматической пожарной

сигнализацией; тревожной сигнализации; системы оповещения и управления эвакуацией.

Оконные конструкции во всех помещениях охраняемого объекта остеклены, имеют надежные и исправные запирающие устройства. На первом этаже объекта защиты установлены пластиковые стеклопакеты. Оконные конструкции обеспечивают надежную защиту помещений объекта и обладают достаточным классом защиты к разрушающим воздействиям. Выделенное помещение, кабинет директора, находится на втором этаже. Окно кабинета смотрит на жилой дом, расположенный в 40 м, через дорогу с интенсивным движением.

На объекте защиты в выделенном помещении – кабинете директора – имеются объекты ОТСС и ВТСС. К ОТСС относятся ПЭВМ и СИДР, ВТСС включает в себя 1 телефон ГАТС, 1 телефон ВАТС и ОПС. Также на объекте расположены системы центрального отопления, энергоснабжения и вентиляции. Планы этажей показаны на рисунках 18.1 и 18.2.

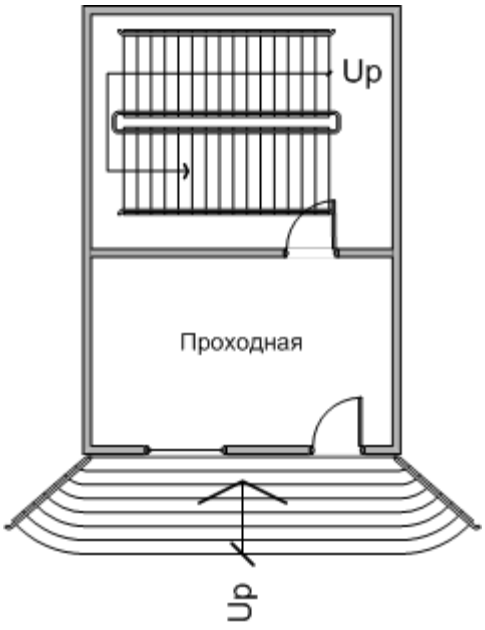


Рисунок 18.1– План первого этажа

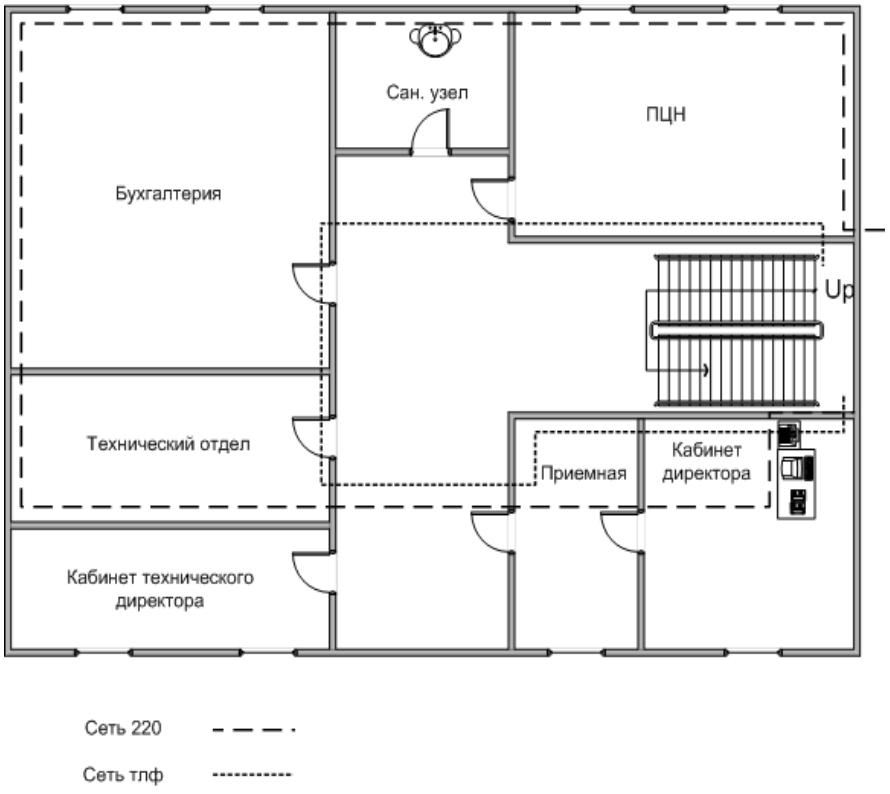


Рисунок 18.2 – План второго этажа

Описание объекта 2. Объект защиты – лаборатория испытания топлив – одно из подразделений исследовательского института. Получение образцов контролируется начальником лаборатории, образцы хранятся в специальных вытяжных шкафах в помещении для хранения образцов топлив (R4). Лабораторные исследования ведутся в трех лабораторных боксах (R1.1, R1.2, R1.3), в которых установлены лабораторные установки различных типов, оснащенные электронными запоминающими устройствами, несколько раз в секунду фиксирующими все показания датчиков установок, а также вспомогательное оборудование. С помощью специального интерфейсного устройства информация переносится на компьютер начальника лаборатории, где происходит ее обработка и готовятся отчеты об испытаниях. Для обслуживания оборудования в лаборатории предусмотрено специальное помещение (R2), в котором имеются средства для электронной диагностики и ремонта лабораторных установок и вспомогательного оборудования.

На всех окнах лаборатории имеются жалюзи, установлена сигнализация (срабатывает при открытии или ударе). Двери в лаборатории деревянные, с огнеупорным покрытием. Наружные двери усилены металлом. Западная стена в помещениях R8, R9 является смежной со стеной основного здания института. Соседние помещения – архивное, для хранения различной документации института (R8), и склад вспомогательных материалов института (R9). Стены кирпичные. В лаборатории две системы приточной вентиляции, для основных и вспомогательных помещений, отдельные вытяжные системы для лабораторных боксов, помещения для техобслуживания лабораторного оборудования (R2) и лабораторных шкафов для хранения лабораторных образцов (в помещении R4). Трубы отопления идут по периметру лаборатории, и через угол кабинета начальника проходят в основное здание института. В кабинете начальника установлен аппарат внутренней телефонной связи. Имеется две ПЭВМ - в кабинете начальника лаборатории и в помещении техобслуживания лабораторного оборудования. Компьютер начальника лаборатории подключен к локальной вычислительной сети института. Планы объекта представлены на рисунках 18.3 и 18.4

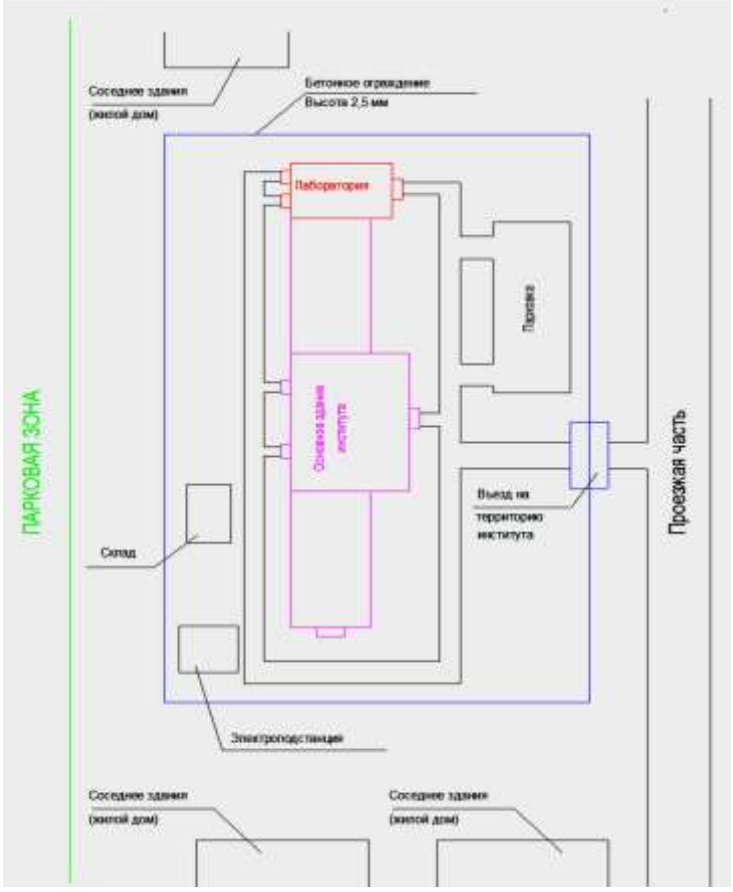


Рисунок 18.3 – План прилегающей территории

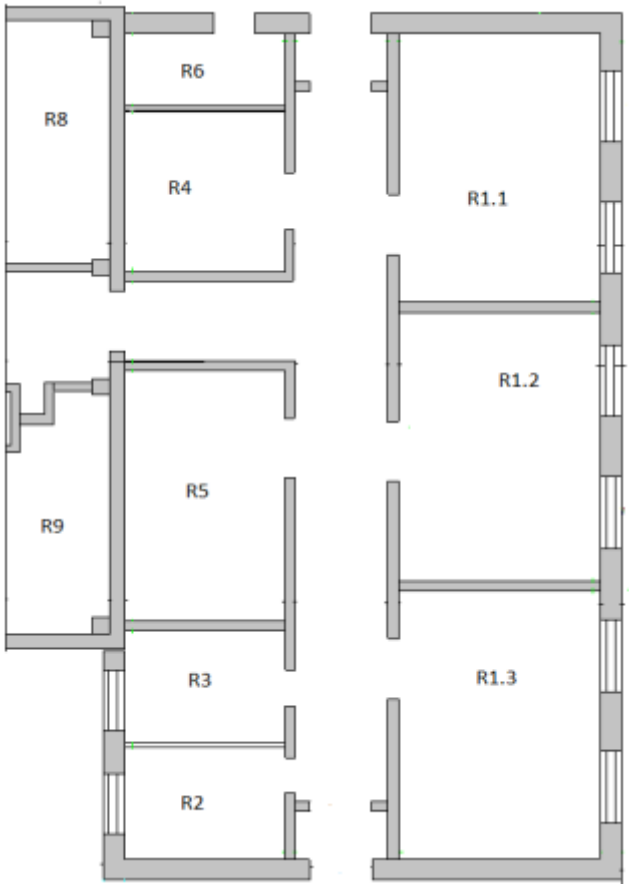


Рисунок 18.4 – План лаборатории

Описание объекта 3. Описание объекта: офис фирмы ComTel, выполняющей проектные работы, расположен на первом этаже офисного здания, вокруг которого расположены жилые дома, автостоянка и магазины. Окна офиса имею двойные рамы; окно выделенного помещения, кабинета директора, выходит на жилые дома. На каждом окне офиса установлены герконовые датчики реагирующие на удар. Двери железные (входная и в кабинет директора) и деревянные (все остальные). Помещение над потолком – магазин радиодеталей, помещение под полом – подвал, соседние помещения отсутствуют. Вентиляция расположена вдоль стены, выходящей на автостоянку; трубы прямоугольного сечения проходит через прихожую, туалет, коридор и кухню. Батареи отопления проходят вдоль восточной стены через бухгалтерию, рабочие комнаты и кабинет директора фирмы; уходят на 2-й этаж и в подвал. В офисе есть цепи электропитания, 5 телефонов внутренней связи и городской телефон в кабинете директора. В кабинете работников есть телевизор. В офисе 6 ПЭВМ: 3 - в

кабинетах работников, 2 - в бухгалтерии, 1 - в кабинете директора. Компьютеры соединены в локальную сеть, в кабинете директора компьютер имеет выход в Интернет.

План прилегающей территории и план офиса показаны на рисунках 18.5 и 18.6.

Рисунок 18.5 – План офиса

Рисунок 18.6 – План территории

Описание объекта 4. Описание объекта защиты: ЗАО «ТД Корвет», занимающееся оптовой торговлей продуктов питания. Фирма расположена в кирпичном двухэтажном здании, две стороны которого выходят на дорогу. Две остальные стороны выходят во внутренний двор банка «Социнвест». На крышу здания можно попасть только со 2 этажа здания (пожарные лестницы отсутствуют). Подвал здания не имеет выход на улицу, он полностью огражден от прохождения широких канализационных трактов и хорошо забетонирован (это здание было частью банка). На всех окнах здания фирмы расположены датчики на открытие и внешнее воздействие, есть жалюзи. Окна кабинетов директоров

зарешечены. Вход в фирму, подсобное помещение, подсобное помещение № 2 и бухгалтерию закрывают железные двери, остальные внутренние двери деревянные. Соседним помещением является коридор, здания банка , толщина стен не менее 30 см. Вентиляция приточная; воздуховод для кондиционера расположен в отделе поставок. Батареи отопления размещены вдоль окон, выходят в подвал в общий стояк. Цепи питания розеток подключены через внутренний электрощит с защитными фильтрами в общий силовой кабель. 15 телефонов организации подключены к мини-АТС. 16 ПЭВМ соединены в локальную сеть; 2 компьютера отдела логистики, 2 компьютера отдела маркетинга и компьютеры директоров имеют выход в интернет. Вход в здание и область приемной охраняется охранником.

План размещения отделов организации показан на рисунках 18.7 и 18.8.

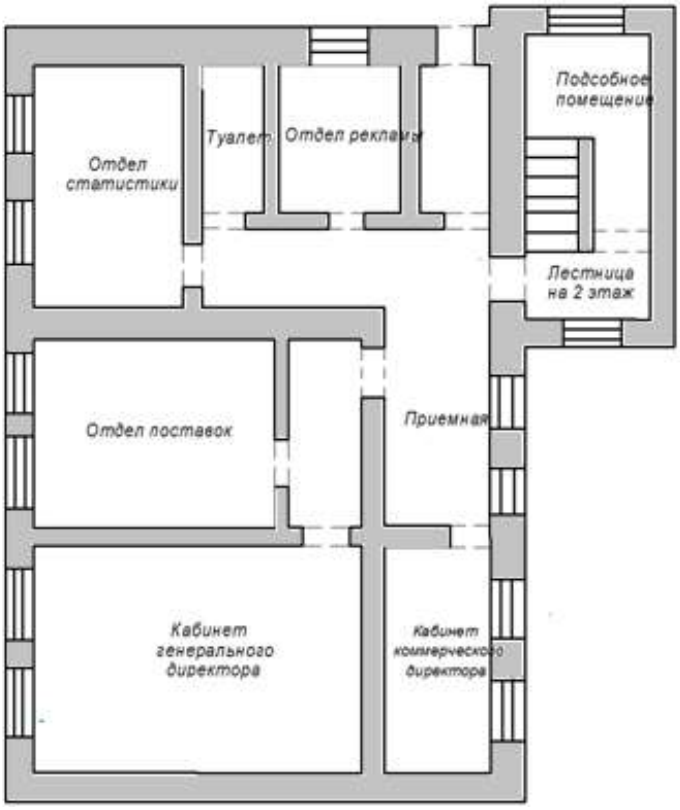


Рисунок 18.7 – План 1-го этажа

Рисунок 18.8 – План 2-го этажа

Описание объекта 5. Описание объекта защиты: компания, предоставляющая Интернет услуги; предоставление доступа к сети Интернет (для этой деятельности отведено специальное помещение – серверная, в которой находится постоянно работающий сервер); предоставление услуги web money –

перевод «реальных» денежных единиц в «виртуальные», на которые затем пользователь может совершать покупки через сеть Интернет. Офис компании находится на третьем этаже трехэтажного здания, вокруг которого расположены жилые дома, торговый комплекс, магазин и ночной клуб. Окна представляют собой двойные пластиковые стеклопакеты, на всех окнах жалюзи. В офис с лестницы установлена стальная дверь, двери в помещения фирмы деревянные, металлическая усиленная с кодовым замком установлена в серверную. Помещение над потолком отсутствует; на втором этаже здания расположены офисные помещения, перекрытием служат железобетонные плиты. Батареи отопления расположены вдоль окон, уходят на 2-й этаж, все трубы выведены через подвал в теплоцентраль. Цепь электропитания фирмы подключена к городской сети, центрального входа в помещении находится электрический щиток. В организации 18 телефонов управляемых мини-АТС; 14 ПЭВМ, все компьютеры имеют доступ к сети Internet , а также входят в состав локальной сети.

План офиса и прилегающей территории показан ниже на рисунках 18.9 и 18.10

Рисунок 18.9 – План офиса

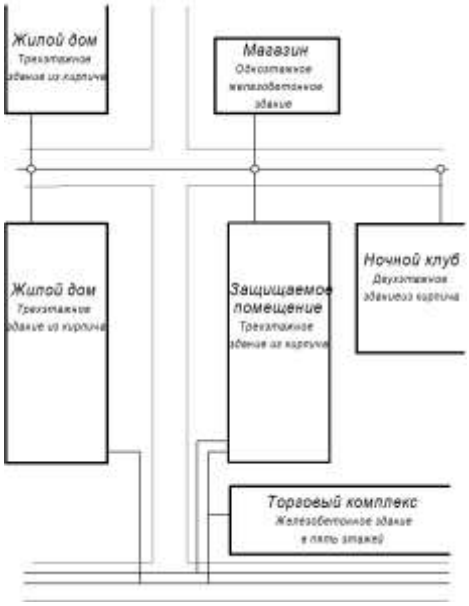


Рисунок 18.10 – План прилегающей территории

Описание объекта 6. Описание объекта защиты: основное направление деятельности ООО «Консалт» – проведение различного рода аудиторских проверок и исследований финансовых учреждений.

Фирма занимает часть первого этажа девятиэтажного жилого дома, окруженный на расстоянии 30-40 метров такими же жилыми домами. В помещении офиса проведены внутренние линии контура питания, внутренней АТС и локальной сети для ПЭВМ. Все окна офиса фирмы пластиковые, тройного остекления. На входе в организацию установлена железная дверь, повышенной прочности, двери внутри помещения деревянные. Непосредственно к офису примыкают внутренние охраняемые гаражные боксы. Под офисом находится подвал жилого здания с общедомовыми коммуникациями (отопление, водоснабжение и другие), доступ в подвал осуществляется через холл жилого дома и постоянно охраняется. Над офисом располагаются жилые квартиры. В здании предусмотрена система центрально-потолочного кондиционирования, компрессоры системы находятся на первом и последних этажах, по дому проложены каналы воздуховодов; система централизованного отопления, радиаторы отопления – чугунные, в офисе находятся под каждым окном.

В здании проложены кабель-каналы, по которым идут провода внутреннего контура силового питания, внутренней локальной сети (ЛВС) и внутренней АТС.

Управления АТС и ЛВС осуществляется с сервера, расположенного в комнате группы технического обеспечения. В помещении офиса есть в наличии: телевизор, система «дом. Кинотеатр» (кабинет руководства); музыкальные центры (кабинеты групп аудита). Локальная сеть насчитывает 18 ПЭВМ и имеет выход в Интернет. Особо защищаемые помещения (архив и хранилище документов и кабинет руководства) подключены к «тревожной кнопке милиции». План защищаемого объекта представлен на рисунке 18.11.

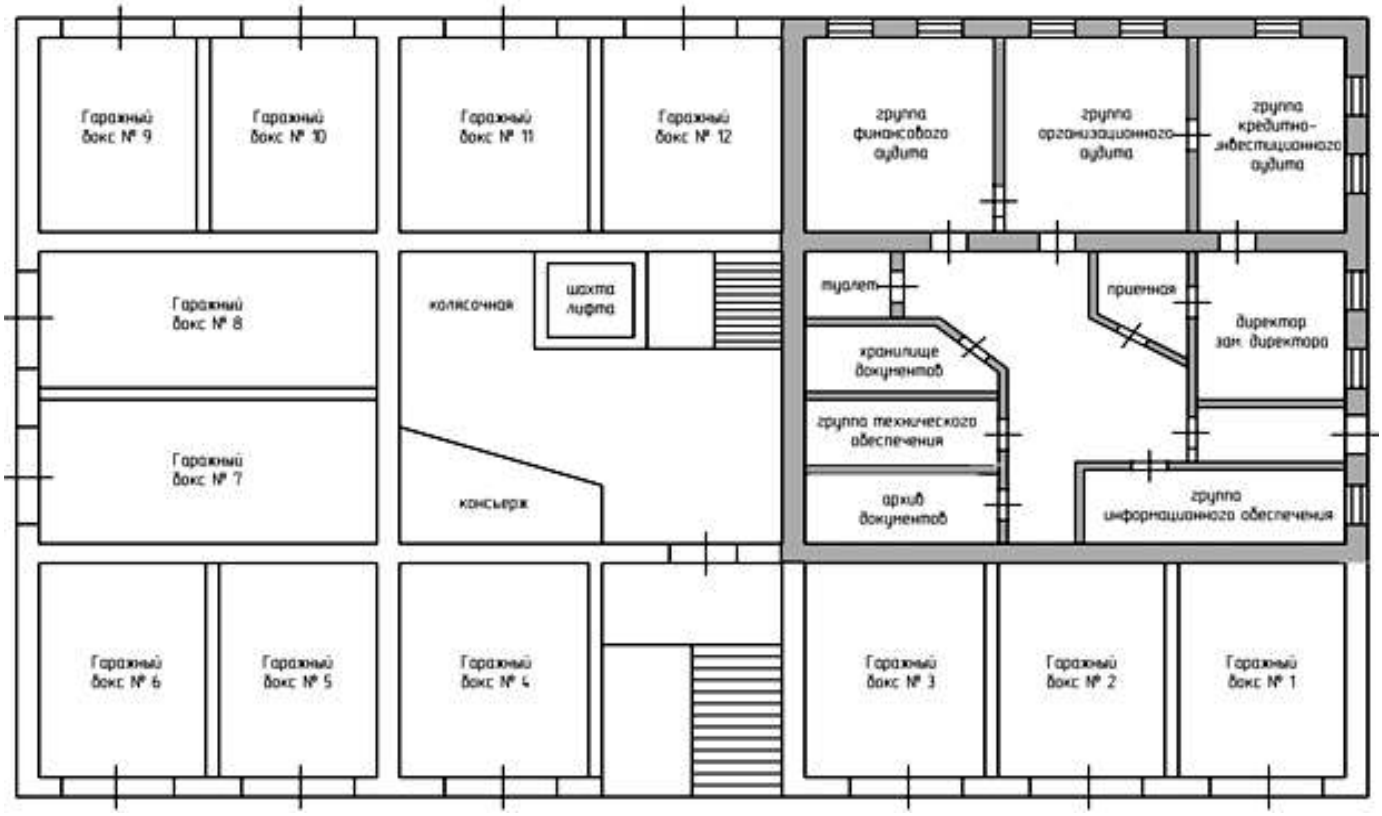


Рисунок 18.11 – План первого этажа здания

Описание объекта 7. Описание объекта защиты: ОАО «Интерком», занимающееся оптовой торговлей компьютерной техники. Фирма расположена в кирпичном одноэтажном здании, две стороны которого выходят на дорогу. Две остальные стороны выходят во внутренний двор, на территории которого расположена автостоянка для сотрудников и склад компьютерной техники. Две стороны склада также выходят на дорогу.

Подвал здания не имеет выход на улицу, он полностью огражден от прохождения широких канализационных трактов и хорошо забетонирован. Все окна здания фирмы имеют тройное остекление, есть жалюзи. Окна кабинета

директора, серверной и окна выходящие на улицу имеют решетки. Вход в офис, серверную, бухгалтерию и кабинет директора закрывают железные двери, остальные внутренние двери деревянные. Двери тамбура и склада двойные распашные, железные, повышенной прочности. Вентиляция приточная; воздуховод для кондиционера расположен в кабинете менеджеров. На складе и офисе установлена система централизованного отопления, имеющая выход за пределы организации. Батареи отопления размещены вдоль окон, выходят в подвал в общий стояк.

Цепи питания розеток подключены через внутренний электрощит с защитными фильтрами в общий силовой кабель. 10 телефонов организации подключены к мини-АТС. 11 ПЭВМ соединены в локальную сеть, имеют выход в интернет. Вход на территорию охраняется постом. Въезд и вход на территорию осуществляется строго по пропускам (для сотрудников). Для посетителей на вход выписывается разовый пропуск, для пропуска на въезд необходимо предъявить документы об оплате товара.

План размещения отделов организации показан на рисунке 18.12.

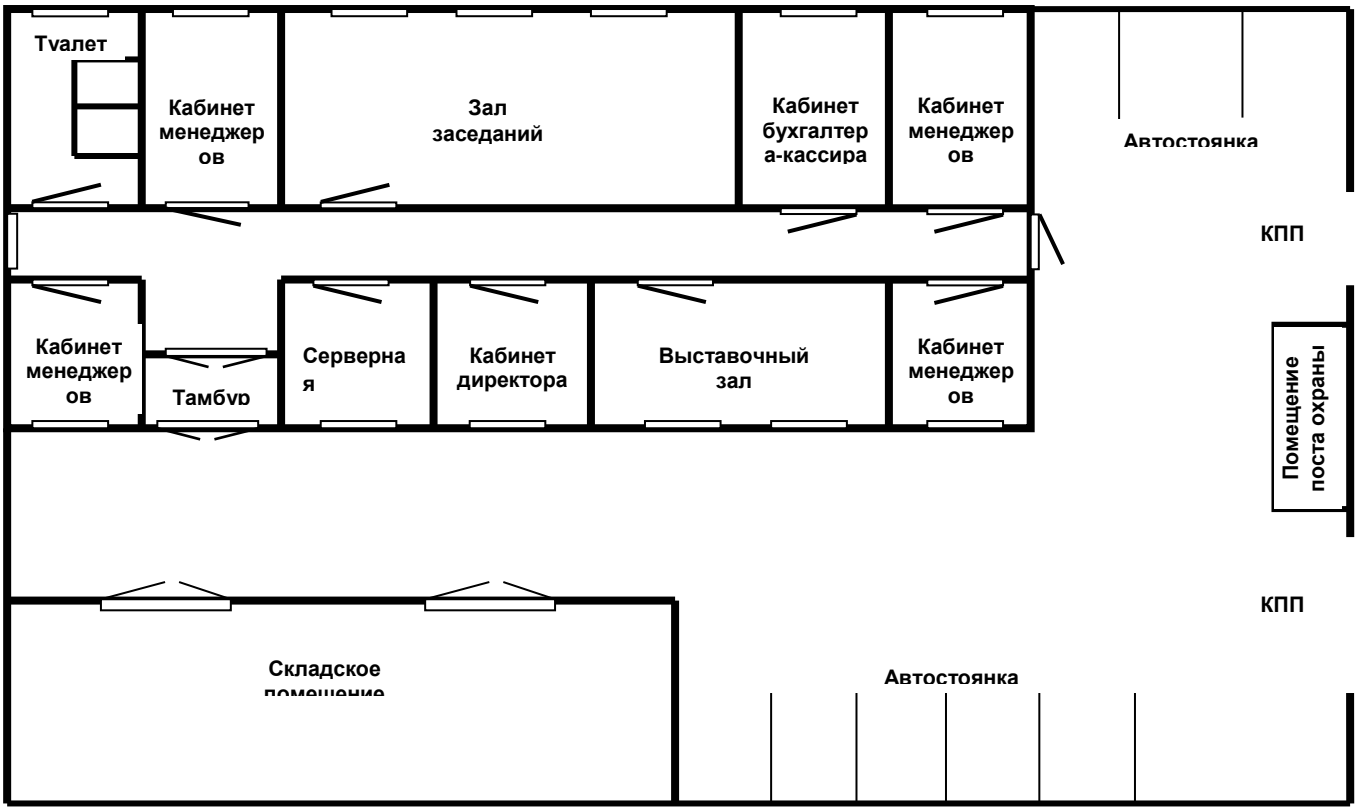


Рисунок 18.12 – План отделов организации

ПРИЛОЖЕНИЕ А

Требования к отчету по практическому занятию

Отчет по практическому занятию должен включать следующие пункты:

- номер и название практической работы;
- дату выполнения;
- цель;
- ответы на вопросы;
- формы документов;

В электронном документе в колонтитуле указывается фамилия, имя студента, номер группы и дата выполнения работы.

Текстовый электронный документ оформляется в соответствии с требованиями ГОСТ 2.105-95. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к текстовым документам (введен Постановлением Госстандарта от 08.08.1995, 426 ред. от 22.06.2006).

Основные требования: цвет шрифта – черный, размер – 14 пт, гарнитура – Times New Roman, начертание – обычное (если не указано иное), выравнивание текста – по ширине, межстрочный интервал – полуторный, размеры полей: левое – 3 см, правое – 1,5 см, верхнее и нижнее – 2 см; абзацный отступ – 1,25 см. Допускается использовать компьютерные возможности акцентирования внимания на определенных терминах, утверждениях применяя различные варианты начертания шрифта.

Более подробно требования расписаны в документе *Требования по оформлению письменных отчетов*.

ДЛЯ ЗАМЕТОК