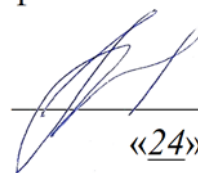


Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

УТВЕРЖДАЮ
Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета



О.Н. Левчegov
«24» апреля 2024 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ ПО ПРОФЕССИОНАЛЬНОМУ
МОДУЛЮ «ПМ.03 ЗАЩИТА ИНФОРМАЦИИ В
ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ
И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ
ЗАЩИТЫ» «ПП.03 ПРОИЗВОДСТВЕННАЯ ПРАКТИКА»**

по специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Фонд оценочных средств разработан на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Черпаков Игорь Владимирович, к.ф.-м.н., доцент кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Фонд оценочных средств рассмотрен и рекомендован к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 23.04.2024 г. №10

Заведующий кафедрой

Учет и информационные технологии в бизнесе _____ Н.С. Морозова



1. Общие положения

Фонды оценочных средств (далее ФОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу профессионального модуля ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты.

ФОС включают контрольные материалы для проведения текущего контроля и итоговой аттестации в форме экзамена.

ФОС разработаны на основании положений:

- ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем;
- Положения о ФОС Липецкого филиала Финуниверситета;
- программы профессионального модуля ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты.

2. Результаты освоения модуля, подлежащие проверке

| | |
|--------------|---|
| Уметь | У1 – применять технические средства защиты информации; У2 – использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; У3 – использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам; У4 – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами. |
| Знать | З1 – физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; З2 – номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации; З3 – основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам; З4 – номенклатуру применяемых средств охраны объектов, систем видеонаблюдения. |

3. Распределение оценивания результатов обучения по видам контроля

| Наименование элемента умений или знаний | Виды аттестации | |
|--|------------------|--------------------------|
| | Текущий контроль | Промежуточная аттестация |
| У1 – применять технические средства защиты информации; | + | + |
| У2 – использовать средства охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; | + | + |
| У3 – использовать средства защиты информации от несанкционированного съема и утечки по техническим каналам; | + | + |
| У4 – применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности техническими средствами. | + | + |
| З1 – физику возникновения технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; | + | + |
| З2 – номенклатуру и характеристики аппаратуры, используемой для съема, перехвата и анализа сигналов в технических каналах утечки информации; | + | + |
| З3 – основные методы и средства технической защиты информации, номенклатуру применяемых средств защиты информации от несанкционированного съема и утечки по техническим каналам; | + | + |
| З4 – номенклатуру применяемых средств охраны объектов, систем видеонаблюдения. | + | + |

4. Распределение типов контрольных заданий по элементам знаний и умений

| Содержание учебного материала по программе УД | Тип контрольного задания | | | | | | | |
|--|--------------------------|----|----|----|----|----|----|----|
| | У1 | У2 | У3 | У4 | З1 | З2 | З3 | З4 |
| Тема 1.1. Объекты информационной защиты | Т | | Рз | | Рз | | | Пр |
| Тема 1.2. Угрозы информационной безопасности | | Т | Пр | | | Т | | |
| Тема 1.3. Методы инженерно-технической защиты информации | Л | | | Т | | Л | | |
| Тема 1.4 Технические основы добывания и инженерно-технической защиты информации | | Т | | | | | | |
| Тема 1.5 Средства скрытого наблюдения | | | Л | | | | Т | |
| Тема 1.6 Средства перехвата сигналов | | | | Рз | Пр | | | Пр |
| Тема 2.1 Основные теории измерения | Л | | Рз | | | Пр | | |
| Тема 2.2 Измерение тока, напряжения и мощности | | Т | | Т | | | | Пр |
| Тема 2.3. Приборы формирования стандартных измерительных сигналов | | | | | | | Л | |
| Тема 2.4 Исследование формы сигналов | Л | | | | | | | |
| Тема 2.5 Измерение параметров сигналов | | Рз | | Л | | | | Т |
| Тема 2.6 Измерение параметров и характеристик электрорадиотехнических цепей и компонентов. | Л | | | | | Пр | | |

Т – тест

Пр – практические работы

Л – лабораторные работы

Рз – решение задачи

5. Распределение типов и количества контрольных заданий по элементам знаний и умений, контролируемых на промежуточной аттестации

| Содержание учебного материала по программе УД | Тип контрольного задания | | | | | | | |
|--|--------------------------|----|----|----|----|----|----|----|
| | У1 | У2 | У3 | У4 | З1 | З2 | З3 | З4 |
| Тема 1.1. Объекты информационной защиты | Э | | | | | | | |
| Тема 1.2. Угрозы информационной безопасности | | Э | | | Э | | | |
| Тема 1.3. Методы инженерно-технической защиты информации | Э | | Э | | | Э | | Э |
| Тема 1.4 Технические основы добывания и инженерно-технической защиты информации | Э | | | Э | | | Э | Э |
| Тема 1.5 Средства скрытого наблюдения | | Э | Э | | Э | | | Э |
| Тема 1.6 Средства перехвата сигналов | Э | | Э | Э | | Э | | Э |
| Тема 2.1 Основные теории измерения | Э | | | | Э | Э | Э | Э |
| Тема 2.2 Измерение тока, напряжения и мощности | | Э | | Э | | | | |
| Тема 2.3. Приборы формирования стандартных измерительных сигналов | | | Э | | Э | | | |
| Тема 2.4 Исследование формы сигналов | Э | | | Э | | Э | Э | |
| Тема 2.5 Измерение параметров сигналов | | Э | | | | | | Э |
| Тема 2.6 Измерение параметров и характеристик электрорадиотехнических цепей и компонентов. | Э | | Э | | | | | |

Э - экзамен

6. Содержание контрольных заданий

Банк тестовых заданий

Задание 1. Расшифруйте аббревиатуру СКУД:

- А. Система контроля и управления доступом;
- Б. Система катализации и управления доступом; В. Система карт и управления доступом;
- Г. Система КПП и удержания диверсантов.

СКУД по среднему количеству емФОСтИ точек доступа

Задание 2.

обычно содержит:

- А. от 32 до 64 точек доступа; Б. от 16 до 64 точек доступа; В. от 50 до 100 точек доступа; Г. от 100 до 300 точек доступа.

Задание 3. СКУД обычно интегрируется...

- А. С системой видеонаблюдения и системой охранно-пожарной сигнализации; Б. С системой вентиляции на предприятии;
- В. С системой охранной;
- Г. С системой пожарной.

Задание 4. Устройством, преграждающим управляемым (УПУ), нельзя назвать

- А. Проходные шлюзы;
- Б. Проходные кабины;
- В. Откатные ворота;
- Г. Дверь с навесным замком; Д. Шлагбаум.

Задание 5. Если СКУД идентифицируется по карточке и отпечатку пальца, то он классифицируется как:

- А. Многоуровневый; Б. Двухступенчатый. В. Одноуровневый Г. Одноступенчатый

Задание 6. Главным отличием автономных СКУД от сетевых (централизованных) является:

- А. Автономные могут функционировать без центрального пульта охраны; Б. Количество точек на предприятии;
- В. Сетевой может обходиться без блока питания.

Задание 7. К каким УПУ относится кабина проходная?

- А. частичным перекрытием;
- Б. с полным перекрытием;
- В. с блокированием объекта в проеме.

Задание 8. Идентификация - это ...

- А. процесс распознавания субъекта (объекта) по присущему или присвоенному ему идентификационному признаку;
- Б. процесс проверки принадлежности субъекту (объекту) доступа предъявленного им (подтверждение подлинности);
- В. процесс идентификации объекта по биометрическим признакам.

Задание 9. Аутентификация - это...

- А. процесс проверки принадлежности субъекту (объекту) доступа предъявленного им аутентификатора (подтверждение подлинности);
- Б. Верификация устройств по MAC-адресу;
- В. процесс проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Задание 10. УВИП- это...

- А. Устройства ввода идентификационных признаков;
- Б. Упорядоченный ввод идентификационных признаков; В. Устройства ввода идентификационных персон.

Задание 11. К достоинствам УВИП на базе идентификаторов Touch Memory НЕ относится:

- А. высокая степень механической и электромагнитной защищённости;
- Б. малые размеры, удобство хранения;

В. возможность обмена данными с компьютером через различные устройства ввода-вывода (пример интерфейс SCSI).

Задание 12. Что не относится к идентификаторам типа eToken?

- А. малые размеры, удобство хранения;
- Б. отсутствие аппаратного считывателя;
- В. простота подсоединения к USB-порту;
- Г. можно использовать как флэш-накопитель.

Задание 13. Металлоискатель (металлодетектор) — электронный прибор...

- А. позволяющий обнаруживать металлические предметы в нейтральной или слабопроводящей среде за счёт их проводимости;
- Б. позволяющий обнаруживать металлические предметы в сильнопроводящей среде за счёт их проводимости;
- В. позволяющий обнаруживать металлические предметы в нейтральной или слабопроводящей среде за счёт видимости;

Задание 14. Принцип работы металлодетекторов основан на А. на возникновении в металле под действием электромагнитного поля индукционных микротоков (токов Фуко);

- Б. на возникновении в металле под действием сверхчастотного акустического воздействия на металлические объекты;
- В. на возникновении в металле под действием электромагнитного поля индукционных микротоков (токов постоянных).

- А. Высокая пропускная способность;
- Б. Низкая вероятность ложной тревоги; В. Компактность;
- Г. Простота использования.

- А. Высокая стоимость;
- Б. Подверженность влиянию помех от различных электроприборов (ламп дневного освещения, электромоторов и т.п.);
- В. Проблема установки нескольких детекторов в один ряд из-за взаимного влияния, вызванного ограниченным диапазоном частот;
- Г. Неоднородность электромагнитного поля, приводящая к возникновению «слепых» зон.

А. Простоте конструкции и невысокой стоимости изготовления;

Задание 15. Главное преимущество арочного металлодетектора перед ручным – это

Задание 16. Принцип импульсной индукции с использованием мультисигментного сигнала и анализом характеристик металла имеет единственный недостаток:

Задание 17. Главное преимущество принципа “приема-передачи” гармонического сигнала заключается в ...

Б. Подверженности влиянию помех создаваемых крупными металлическими объектами поблизости;

В. Отсутствию обнаружения объектов из цветных металлов

А. Подборка кадров;

Б. Формирование службы эксплуатации;

В. Обучение обслуживающего персонала правилам эксплуатации систем;

Г. разработка практических мер и сценариев действий службы безопасности и сотрудников предприятия при штатных и нештатных ситуациях; Д. Все выше перечисленное входит в этап подготовки персонала.

А. пассивный метод магнитометрии, основанный на определении малых аномалий интенсивности магнитного поля Земли;

Б. метод уравновешенной индукции;

В. принцип “приема-передачи” гармонического сигнала с анализом амплитуды и фазового сдвига принимаемого сигнала;

Г. принцип импульсной индукции с использованием импульсного сигнала,

- Задание 18. В подготовку персонала на этапе проектирования ТСО не включается
- Задание 19. Укажите принцип, на котором основан самый надежный тип арочного металлодетектора
- анализом амплитуды и времени затухания;
- Д. принцип импульсной индукции, с использованием импульсного сигнала и анализом характеристик металла.
- А. Цифровых системах видеонаблюдения; Б. Аналоговых системах видеонаблюдения; В. В сетевых системах видеонаблюдения.
- мультисигментного
- Задание 20. Коаксиальные провода в линиях связи преимущественно преобладают в...
- Задание 21. Какая характеристика систем видеонаблюдения не относится к аналоговым?
- А. низкая цена прокладки линии передачи данных Б. высокая стабильность сигнала
- В. малая масса и габариты камер
- Г. низкая цена камер
- Задание 22. Выберите верный порядок функционирования системы видеонаблюдения:
- А. Камера – Блок обработки – Монитор – Наблюдатель Б. Наблюдатель – Монитор – Блок обработки – Камера В. Блок обработки – Монитор – Камера Наблюдатель
- Задание 23. Укажите тип матрицы видеокамер, который сейчас не пользуется популярностью на рынке
- А. ПЗС;
- Б. КМОП. В. CMOS
- Задание 24. Маленькие фокусные расстояния (f) в камерах видеонаблюдения характерны для:
- А. Широкого угла обзора; Б. Узкого угла обзора;
- В. Среднего угла обзора.
- А. Благодаря ИК подсветке можно распознать объекты в полной темноте; Б. Длина волны ИК излучения 800-950 нм отлично различима для человеческих глаз;
- Задание 25. Выберите ложное утверждение:
- В. Дальность обнаружения с ИК подсветкой обычно 10-80 метров (в действительности не более 20 метров).
- А. Автоматически подстраиваться под условия освещения, регулируя количество света, проходящего через диафрагму;
- Б. Автоматически поворачивать камеру, благодаря автофокусировке изображения;
- В. Автоматически распознавать характерные формы лица человека.
- Задание 26. Автодиафрагма (АРД) в камере видеонаблюдения позволяет:
- Задание 27. Исследования окружающего пространства с помощью звуковых волн, не распознаваемых для человека характерно для ...
- А. ИК датчиков движения; Б. УЗ датчиков движения; В. СВЧ датчиков движения.
- А. Телевизионными линиями (ТВЛ);
- Б. Количеством пикселей;
- В. Плотностью пикселей на дюйм (dpi).
- А. Люксах;
- Б. Фотонов на микрон в квадрате; В. Флюксах.
- Задание 28. Разрешение для аналоговых видеокамер измеряется...
- Задание 29. Чувствительность камеры видеонаблюдения измеряется в...
- Задание 30. Для ночной освещенности объектов характерно следующее количество люкс:
- А. <4 люкс;
- Б. <500 люкс;
- В. <100-200 люкс.
- Задание 31. Матрица в камере - это...
- А. совокупность ячеек, способных передавать информацию о свете;

Б. набор вертикальных Y и горизонтальных (условно) X линий (проводников), с возможностью замыкания в точках их пересечений, выводы которых подключены к выводам контроллера, который осуществляет их периодический опрос;

В. название специального диска, служащий образцом для создания дисков (компактдиск, DVD и др.) с записью (музыки, файлов).

Задание 32. В этап предпроектной работы не входит

А. проводится обследование и изучение функционирования объекта с точки зрения его безопасности;

Б. выполняются аналитические работы по оценке угроз, выделению по степени важности отдельных зон;

В. разработка модели нарушителя и выбору схемы взаимодействия технических средств защиты и личного состава охраны;

Г. тестирование системы

Задание 33. Датчик движения – это...

А. это устройство для получения информации о состоянии контролируемой им системы, преобразующее данные об изменении характеристик исследуемой области в сигнал, удобный для дальнейшего использования;

Б. устройство тревоги систем управления и доступа контроля на предприятии. В. программно-аппаратное устройство, выполненное в виде купола и предназначено для контроля защищаемых помещений (ЗП).

А. Система Граничного Подавления;

Б. Система Газового Подавления;

В. Система Гарантированного Подавления.

А. "АЛГОГЕН"; Б. "Циклон Б"; В. "Газваген".

Задание 34. СГП - это...

Задание 35. Главным действующим веществом в СГП "Армагеддон" является...

Задание 36. В СГП "Армагеддон" не входит... (выберите правильный ответ)

А. Устройства постановки/снятия;

Б. Центрального блока;

В. Комплекта пиропатронов;

Г. Датчиков о вторжении в зону и мощной сирены; Д. Контроллер СКУД.

А. Глаза;

Б. Носоглотка и дыхательные пути; В. Кожа;

Г. Органы слуха.

А. 15 мин - 30 мин; Б. 30 мин - 45 мин; В. 45 мин - 60 мин.

Задание 39. СГП "Армагеддон" характеризуется как система... А. летального действия;

Б. нелетального действия;

В. полулетального действия.

Задание 40. ТСВ - это...

А. Технические Средства Воздействия;

Б. Технологические Средства Воспрещения; В. Техника Средств Восприятия.

Задание 41. ЭМИ-пушки основаны на принципе...

А. На основе ЭМИ — электромагнитного импульса;

Б. На основе ЭМИ — Электро Магнитизма Исполнения;

В. На основе ЭМИ — Элементарного Магнитного Импульса.

Задание 42. Назначение ЭМИ-пушек -- ...

А. Предназначены для принудительной остановки транспортных средств, при помощи высокоэнергетических импульсов микроволнового излучения; Данные устройства дистанционно воздействуют на электронную бортовую аппаратуру;

- Б. Предназначены для дистанционного облучения помехами электронную бортовую аппаратуру противника;
- В. Предназначены для вывода из строя экипажа противника под действием ЭМИ-лучей на биологические объекты.
- А. Ослепления лазерным лучом;
- Б. Подача тревожного сигнала;
- В. Вывод лучами ЭМИ аппаратуры противника.
- А. Данное устройство содержит высокоэнергетические композиции, формирующие аэрозольные облака из специального состава, рецептура которых может содержать углеводородные топлива и металлы с высокой температурой сгорания, суперокислители и другие компоненты;
- Б. Роботизированное устройство активно подавляет и устраняет двигательные установки ТС посредством выстрелов огнестрельных патронов летального действия, что может не только вывести из строя технику, но и уничтожить экипаж;
- Задание 43. Прототипы лазерного устройства «Поток», Lazer Dazzler и PNaSR используются для...
- Задание 44. SGR-1 Выберите характеристику TCB SGR-1:
- В. Данное устройство содержит химические реагенты, которые временно парализуют персонал посредством распыления аэрозоля, принцип работы схож с СПП «Армагеддон».
- А. электризуемые ограждения на основе напряжения приФОСновения
- Задание 45. К электрошоковым устройствам (ЭШУ), воздействующим на живую силу электрическим током, НЕ относятся:
- (воздействующие импульсными высоковольтными разрядами электрического тока);
- Б. Электризуемые ограждения на основе шагового напряжения и неконтактной электризации;
- В. Тайзеры;
- Г. устройства с применением плазменного газодисперсного или водяного электропроводящего канала;
- Д. устройства на основе генерации электромагнитной газовой плазмы.
- Задание 46. Средства, ограничивающие подвижность можно отнести к ... А. самым действенным средствам;
- Б. самым нелетальным средствам;
- В. самым летальным средствам.
- А. специальные сети;
- Б. автозаградители;
- В. автоблокираторы;
- Г. устройства, генерирующие пенновязущие составы; Д. спецклеи;
- Е. ручные гранаты.
- Задание 47. К средствам, ограничивающим подвижность живой силы и транспортных средств, не относятся:
- Задание 48. Кинетические средства можно отнести к самым... А. Летальным средствам воздействия;
- Б. Нелетальным средствам воздействия;
- В. Тяжелым средствам воздействия.
- Задание 49. Обеспечение безопасности и охраны объектов не осуществляется подразделениями:
- А. государственной, ведомственной, вневедомственной охраны; Б. частными охранными предприятиями;
- В. сторожами собственной службы охраны организаций;
- Г. техническими средствами охраны;
- Д. нечастными охранными предприятиями.
- Задание 50. Главной целью охраны предприятия НЕ является:

- А. предотвращение попыток проникновения посторонних лиц (злоумышленников) на территорию (объекты) предприятия;
- Б. обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию;
- В. своевременное обнаружение и задержание лиц, противоправно проникших (пытающихся проникнуть) на охраняемую территорию;
- Г. предупреждение происшествий на охраняемом объекте и ликвидация их последствий;
- Д. Установка и поддержание требований пожарной безопасности.

Задание 51. Система охраны предприятия - это...

- А. совокупность используемых для охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов;
- Б. система средств, а также способов и методов охраны предприятия и его объектов;
- В. система физического и технического контроля объектов защиты от злоумышленников.

Задание 52. Ведомственная охрана - это...

- А. совокупность создаваемых имеющими право на создание ведомственной охраны федеральными органами исполнительной власти и организациями органов управления, сил и средств, предназначенных для защиты охраняемых объектов от противоправных посягательств;
- Б. государственное полицейское подразделение, осуществляющее охрану особо важных и режимных объектов (в том числе подлежащих обязательной охране войсками национальной гвардии), имущества физических и юридических лиц по договорам;
- В. организация, специально учрежденная для оказания охранных услуг, зарегистрированная в установленном законом порядке и имеющая лицензию на осуществление частной охранной деятельности.

А. совокупность создаваемых имеющими право на создание ведомственной охраны федеральными органами исполнительной власти и организациями органов управления, сил и средств, предназначенных для защиты охраняемых объектов от противоправных посягательств;

Б. государственное полицейское подразделение, осуществляющее охрану особо важных и режимных объектов (в том числе подлежащих обязательной охране войсками национальной гвардии), имущества физических и юридических лиц по договорам;

В. организация, специально учрежденная для оказания охранных услуг, зарегистрированная в установленном законом порядке и имеющая лицензию на осуществление частной охранной деятельности.

Задание 54. Частная охранная организация - это

А. совокупность создаваемых имеющими право на создание ведомственной охраны федеральными органами исполнительной власти и организациями органов управления, сил и средств, предназначенных для защиты охраняемых объектов от противоправных посягательств;

Б. государственное полицейское подразделение, осуществляющее охрану особо важных и режимных объектов (в том числе подлежащих обязательной охране войсками национальной гвардии), имущества физических и юридических лиц по договорам;

В. организация, специально учрежденная для оказания охранных услуг, зарегистрированная в установленном законом порядке и имеющая лицензию на осуществление частной охранной деятельности.

Задание 55. Какое выражение истинно?

А. Сертификация возможна только ОИ (объектов информатизаций);

Б. Аттестация возможна только СЗИ (средств защиты информации);

В. Сертификация возможна только СЗИ (средств защиты информации).

Задание 56. РСП – это...

А. Режимное-Секретное Подразделение; Б. Российский Секретный Патруль;

В. Репутационный Секторный Полк.

Задание 57. Отдел СП – это...

А. Отдел специальных проверок; Б. Отдел специальных проектов; В. Отдел секретных проектов.

Задание 58. Отдел СИ – это...

А. Отдел специальных исследований; Б. Отдел специальных инструкций; В. Отдел секретных инструкций.

Задание 59. Специальная проверка – это...

А. проверка оборудования и технических средств на отсутствие каких-либо скрытых устройств, предназначенных для негласного прослушивания, записи, перехвата и передачи информации;

Б. проверка помещений на отсутствие каких-либо скрытых устройств, предназначенных для негласного прослушивания, записи, перехвата и передачи информации;

В. проверка как и помещений так и аппаратуры на отсутствие устройств негласного перехвата информации.

Задание 60. Специальное исследование – это...

А. комплекс действий, направленный на ОБНАРУЖЕНИЕ потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России;

Б. комплекс действий, направленный на ЛИКВИДИРОВАНИЕ потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

В. комплекс действий, направленный на ОБОСНОВАНИЕ потенциальных технических каналов утечки защищаемой информации с помощью специального контрольно-измерительного оборудования, в соответствии с нормативно-методическими документами ФСБ России и ФСТЭК России.

Задание 61. Укажите, что из нижеперечисленного не относится к деятельности современной компании по защите гос. тайны

А. Защита информации составляющую государственную, служебную и коммерческую тайны, персональных данных и конфиденциальной информации;

Б. Подготовка предприятий к лицензированию отдельных видов деятельности; В. Аттестация объектов информатизаций;

Г. Аутентификация объектов информатизации;

Д. Специальные проверки и специальные исследования технических средств; Е. Строительство и реконструкция специальных объектов и объектов общего назначения;

Ж. Сертификационные испытания и измерения в собственной электролаборатории.

№ 1 2 3 4 5 6 7 8 9 10 11 12 13 задания

Ответ А Б А Г А А В А В А В Г А

№ 14 15 16 17 18 19 20 21 22 23 24 25 26 задания

Ответ А А А А Д Д Б В А А А Б А

№ 27 28 29 30 31 32 33 34 35 36 37 38 39 задания

Ответ Б А А А А Г А Б А Д Г Б Б

№ 40 41 42 43 44 45 46 47 48 49 50 51 52 задания

Ответ А А А А А Д Б Е Б Д Д А А

№ 53 54 55 56 57 58 59 60 61 задания

Ответ Б В В А Б А А А Г

Перечень практических занятий

- Практическое занятие No1. Анализ бизнес-требований к информационной безопасности
- Практическое занятие No2. Анализ бизнес-требований к информационной безопасности (продолжение)
- Практическое занятие No3. Разработка концептуального плана защиты.
- Практическое занятие No4. Разработка концептуального плана защиты. (продолжение)
- Практическое занятие No5. Анализ технических ограничений плана защиты
- Практическое занятие No6. Анализ технических ограничений плана защиты (продолжение)
- Практическое занятие No7. Применение сертификатов для аутентификации и авторизации
- Практическое занятие No8. Применение сертификатов для аутентификации и авторизации (продолжение)
- Практическое занятие No9. Проектирование иерархии ЦС. Практическое занятие No10. Проектирование иерархии ЦС. (продолжение)
- Практическое занятие No11. Проектирование административных ролей ЦС
- Практическое занятие No12. Проектирование административных ролей ЦС (продолжение)
- Практическое занятие No13. Проектирование политики подачи заявок на сертификаты.
- Практическое занятие No14. Проектирование политики подачи заявок на сертификаты. (продолжение)
- Практическое занятие No15. Проектирование размещения CRL и интервала публикации.
- Практическое занятие No16. Проектирование размещения CRL и интервала публикации. (продолжение)
- Практическое занятие No17. Проектирование защиты границ сети. Практическое занятие No18. Проектирование защиты границ сети. (продолжение)
- Практическое занятие No19. Защита DNS. Проектирование политики IPSec.
- Практическое занятие No20. Защита DNS. Проектирование политики IPSec. (продолжение)
- Практическое занятие No21. Сервисы безопасности в вычислительных сетях
- Практическое занятие No22. Сервисы безопасности в вычислительных сетях (продолжение)
- Практическое занятие No23. Администрирование средств безопасности
- Практическое занятие No24. Администрирование средств безопасности (продолжение)
- Практическое занятие No25. Разработка политики информационной безопасности
- Практическое занятие No26. Разработка политики информационной безопасности (продолжение)
- Практическое занятие No27. Каналы несанкционированного доступа к информации
- Практическое занятие No28. Каналы несанкционированного доступа к информации (продолжение)
- Практическое занятие No29. Борьба с компьютерными вирусами Практическое занятие No30. Борьба с компьютерными вирусами (продолжение)
- Практическое занятие No31. Обнаружение загрузочного вируса
- Практическое занятие No32. Обнаружение резидентного вируса Практическое занятие No33. Обнаружение макровируса
- Практическое занятие No34. Изучение протоколов TCP и UDP
- Практическое занятие No35. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO
- Практическое занятие No36. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO (продолжение)
- Практическое занятие No37. Защита распределенных вычислительных сетей
- Практическое занятие No38. Защита распределенных вычислительных сетей (продолжение)
- Практическое занятие No39. Построение защищенной вычислительной сети
- Практическое занятие No40. Построение защищенной вычислительной сети (продолжение)

Перечень вопросов для устного ответа

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
4. Что понимается под "компьютерной безопасностью"?
5. Перечислите составляющие информационной безопасности.
6. Приведите определение доступности информации.
7. Приведите определение целостности информации.
8. Приведите определение конфиденциальности информации.
9. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
10. Перечислите задачи информационной безопасности общества.
11. Перечислите уровни формирования режима информационной безопасности.
12. Дайте краткую характеристику законодательно-правового уровня.
13. Какие подуровни включает программно-технический уровень?
14. Что включает административный уровень?
15. В чем особенность морально-этического подуровня?
16. Перечислите основополагающие документы по информационной безопасности.
17. Понятие государственной тайны.
18. Что понимается под средствами защиты государственной тайны?
19. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
20. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
21. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
22. Какие виды требований включает стандарт ISO/IEC 15408?
23. Чем отличаются функциональные требования от требований доверия?
24. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
25. Какова цель требований по отказоустойчивости информационных систем?
26. Сколько классов функциональных требований?
27. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
28. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
29. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
30. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
31. Показатели защищенности межсетевых экранов.
32. Классы защищенности межсетевых экранов.
33. Цели и задачи административного уровня обеспечения информационной безопасности.
34. Содержание административного уровня.
35. Дайте определение политики безопасности.
36. Направления разработки политики безопасности.
37. Перечислите составные элементы автоматизированных систем.
38. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
39. Перечислите классы угроз информационной безопасности.

40. Назовите причины и источники случайных воздействий на информационные системы.
41. Дайте характеристику преднамеренным угрозам.
42. Перечислите каналы несанкционированного доступа.
43. В чем особенность "упреждающей" защиты в информационных системах.
44. Характерные черты компьютерных вирусов.
45. Дайте определение программного вируса.
46. Какие трудности возникают при определении компьютерного вируса?
47. Когда появился первый вирус, который самостоятельно дописывал себя в файлы?
48. В чем особенность компьютерного вируса "Чернобыль"?
49. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях? Почему?
50. Перечислите классификационные признаки компьютерных вирусов.
51. Охарактеризуйте файловый и загрузочный вирусы.
52. В чем особенности резидентных вирусов?
53. Сформулируйте признаки стелс-вирусов.
54. Перечислите деструктивные возможности компьютерных вирусов.
55. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
56. Перечислите виды "вирусоподобных" программ.
57. Поясните механизм функционирования "троянской программы" (логической бомбы).
58. В чем заключаются деструктивные свойства логических бомб?
59. Как используются утилиты скрытого администрирования и их деструктивные возможности?
60. Охарактеризуйте "intended"-вирусы и причины их появления.
61. Для чего используются конструкторы вирусов?
62. Для создания каких вирусов используются полиморфик-генераторы?
63. Поясните понятия "сканирование налету" и "сканирование по запросу".
64. Перечислите виды антивирусных программ.
65. Охарактеризуйте антивирусные сканеры.
66. Принципы функционирования блокировщиков и иммунизаторов.
67. Особенности CRC-сканеров.
68. В чем состоят особенности эвристических сканеров?
69. Какие факторы определяют качество антивирусной программы?
70. Перечислите наиболее распространенные пути заражения компьютеров вирусами.
71. Какие особенности заражения вирусами при использовании электронной почты?
72. Особенности заражения компьютеров локальных сетей.
73. Перечислите основные правила защиты от компьютерных вирусов, получаемых не из вычислительных сетей.
74. Как ограничить заражение макровирусом при работе с офисными приложениями?
75. Как обнаружить загрузочный вирус?
76. Как обнаружить резидентный вирус?
77. Характерные черты макровируса.
78. Как проверить систему на наличие макровируса?
79. Является ли наличие скрытых листов в Excel признаком заражения макровирусом?
80. Перечислите основные этапы алгоритма обнаружения вируса.
81. Особенности обеспечения информационной безопасности компьютерных сетей.
82. Дайте определение понятия "удаленная угроза".
83. Основные цели информационной безопасности компьютерных сетей.
84. В чем заключается специфика методов и средств защиты компьютерных сетей?
85. Поясните понятие "глобальная сетевая атака", приведите примеры.
86. Что понимается под протоколом передачи данных?
87. Охарактеризуйте сети с коммутацией сообщений и коммутацией пакетов.

88. Чем отличается соединение по виртуальному каналу от передачи датаграмм?
89. Какие протоколы образуют модель TCP/IP?
90. Какие уровни входят в сетевую модель TCP/IP?
91. Дайте характеристику всех уровней модели TCP/IP и укажите соответствующие этим уровням протоколы.
92. Соотнесите по уровням модели TCP/IP понятия "пакет" и "кадр". Чем они отличаются?
93. Какой протокол обеспечивает преобразование логических сетевых адресов в аппаратные?
94. Проведите сравнительную характеристику моделей передачи данных TCP/IP и OSI/ISO.
95. Перечислите уровни модели OSI/ISO.
96. Назначение прикладного и представительного уровней модели OSI/ISO.
97. Какие функции выполняет транспортный уровень?
98. Назначение сетевого уровня и его характеристика.
99. Какие физические устройства реализуют функции канального уровня?
100. В чем особенности физического уровня модели OSI/ISO?
100. На каких уровнях модели OSI/ISO должна обеспечиваться аутентификация?
101. На каком уровне модели OSI/ISO реализуется сервис безопасности "неотказуемость" (согласно "Общим критериям")?
102. Как рассматривается сеть в концепции протокола IP?
103. Что такое IP-адрес?
104. Преобразуйте IP-адрес "11110011 10100101 00001110 11000001" в десятичную форму.
105. Сколько классов сетей определяет IP протокол?
106. Из каких частей состоит IP-адрес?
107. К какому классу относится следующий адрес: 199.226.33.168?
108. Какой из этих адресов не может существовать: 109.256.33.18 или 111.223.44.1? 109. Поясните понятие домена.
110. В чем заключается иерархический принцип системы доменных имен?
111. Для чего предназначен DNS-сервер?
112. Приведите примеры доменов верхнего уровня по географическому признаку 113. Перечислите классы удаленных угроз.
114. Как классифицируются удаленные угрозы "по характеру воздействия"? 115. Охарактеризуйте удаленные угрозы "по цели воздействия".
116. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
117. Дайте определение маршрутизатора.
118. Что такое подсеть и сегмент сети? Чем они отличаются?
119. Может ли пассивная угроза привести к нарушению целостности информации? 120. Дайте определение типовой удаленной атаки.
121. Механизм реализации удаленной атаки "анализ сетевого трафика".
122. Что является целью злоумышленников при "анализе сетевого трафика"? 123. Назовите причины успеха удаленной атаки "ложный объект".
124. Охарактеризуйте удаленную атаку "подмена доверенного объекта" по классам угроз.
125. Поясните возможные механизмы реализации удаленной атаки "отказ в обслуживании".
126. Какие составляющие "информационной безопасности" могут быть нарушены при реализации каждой из типовых удаленных атак?
127. Перечислите основные причины успешной реализации удаленных угроз информационной безопасности в вычислительных сетях.
128. Почему виртуальное соединение не обеспечивает требуемого уровня защиты вычислительных сетей?

- 129.Какая из причин приводит к успеху удаленной угрозы "анализ сетевого трафика"? 130.Что является следствием недостаточной аутентификации субъектов и объектов вычислительных сетей?
- 131.К чему приводит недостаточность информации об объектах вычислительной сети? Приведите пример.
- 132.Может ли быть нарушена целостность информации при отсутствии в распределенных вычислительных сетях возможности контроля за маршрутом сообщений? Почему?
- 133.В чем заключаются преимущества сети с выделенными каналами?
- 134.Какие алгоритмы удаленного поиска Вам известны?
- 135.Какой из алгоритмов поиска более безопасный?
- 136.Как повысить защищенность вычислительных сетей при установлении виртуального соединения?
- 137.Как можно защитить сеть от реализации атаки "отказ в обслуживании"?
- 138.Как можно контролировать маршрут сообщения в сети?
- 139.Что понимается под идентификацией пользователя?
- 140.Что понимается под аутентификацией пользователей?
- 141.Применим ли механизм идентификации к процессам? Почему?
- 142.Перечислите возможные идентификаторы при реализации идентификации.
- 143.Перечислите возможные идентификаторы при реализации механизма аутентификации.
- 144.Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
- 145.В чем особенности динамической аутентификации?
- 146.Опишите механизм аутентификации пользователя.
- 147.Что такое "электронный ключ"?
- 148.Перечислите виды аутентификации по уровню информационной безопасности.
- 149.Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?
- 150.Что входит в состав криптосистемы?
- 151.Какие составляющие информационной безопасности могут
криптосистемы?
- 152.Назовите классификационные признаки методов шифрования данных.
- 153.Поясните механизм шифрования "налету".
- 154.Как реализуется симметричный метод шифрования?
- 155.Как реализуется асимметричный метод шифрования?
- 156.Что понимается под ключом криптосистемы?
- 157.Какие методы шифрования используются в вычислительных сетях?
- 158.Что такое электронная цифровая подпись?
- 159.Какой метод шифрования используется в электронной цифровой подписи?
- 160.Чем определяется надежность криптосистемы?
- 161.Перечислите известные методы разграничения доступа.
- 162.В чем заключается разграничение доступа по спискам?
- 163.Как используется матрица разграничения доступа?
- 164.Опишите механизм разграничения доступа по уровням секретности и категориям.
- 165.Какие методы управления доступа предусмотрены в руководящих документах Гостехкомиссии?
- 166.Поясните механизм дискретного управления доступом?
- 167.Сравните дискретное и мандатное управление доступом.
- 168.На чем основан механизм регистрации?
- 169.Какие события, связанные с безопасностью, подлежат регистрации?
- 170.Чем отличаются механизмы регистрации и аудита?
- 171.Дайте определение аудита событий информационной системы.
- 172.Что относится к средствам регистрации и аудита?

173. Что такое регистрационный журнал? Его форма.
174. Что понимается под подозрительной активностью?
175. Какие этапы предусматривают механизмы регистрации и аудита?
176. Охарактеризуйте известные методы аудита безопасности информационных систем.
177. В чем заключается механизм межсетевого экранирования?
178. Дайте определение межсетевого экрана.
179. Принцип функционирования межсетевых экранов с фильтрацией пакетов.
180. На уровне каких протоколов работает шлюз сеансового уровня?
181. В чем особенность межсетевых экранов экспертного уровня?
182. Какие сервисы безопасности включает технология виртуальных частных сетей?
183. Назовите функции VPN-агента.
184. Каким образом технология VPN обеспечивает конфиденциальность данных?
185. Каким образом технология VPN обеспечивает целостность данных?
186. Почему при использовании технологии VPN IP-адреса внутренней сети недоступны внешней сети?
187. Что такое "туннель" и технология его создания?
188. Чем определяется политика безопасности виртуальной частной сети?

Итоговое тестирование

Задание №1

Физические средства защиты информации

Выберите один из 4 вариантов ответа:

- 1) средства, которые реализуются в виде автономных устройств и систем
- 2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- 3) это программы, предназначенные для выполнения функций, связанных с защитой информации
- 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание №2

Технические средства защиты информации

Выберите один из 4 вариантов ответа:

- 1) средства, которые реализуются в виде автономных устройств и систем
- 2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
- 3) это программы, предназначенные для выполнения функций, связанных с защитой информации
- 4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Задание №3

Утечка информации

Выберите один из 3 вариантов ответа:

- 1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
- 2) ознакомление постороннего лица с содержанием секретной информации
- 3) потеря, хищение, разрушение или неполучение переданных данных

Задание №4

Под изоляцией и разделением (требование к обеспечению ИБ) понимают

Выберите один из 2 вариантов ответа:

- 1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)
- 2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

Задание №5

Виды технической разведки (по месту размещения аппаратуры)

Выберите несколько из 7 вариантов ответа:

- 1) ФОСмическая
- 2) оптическая
- 3) наземная
- 4) фотографическая
- 5) морская
- 6) воздушная
- 7) магнитометрическая

Задание № 6

Основные группы технических средств ведения разведки

Выберите несколько из 5 вариантов ответа:

- 1) радиомикрофоны
- 2) фотоаппараты
- 3) электронные "уши"
- 4) дистанционное прослушивание разговоров
- 5) системы определения местоположения контролируемого объекта

Задание №7

Инженерно-техническая защита –это

Запишите ответ _____

Задание № 8

Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

Выберите один из 4 вариантов ответа:

- 1) угрозой;
- 2) опасностью;
- 3) намерением;
- 4) предостережением.

Задание №9

Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ:

Задание № 10

Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

Выберите один из 4 вариантов ответа:

- 1) операционной системы, сетевого программного обеспечения
- 2) операционной системы, сетевого программного обеспечения и системы управления базами данных;
- 3) операционной системы, системы управления базами данных;
- 4) сетевого программного обеспечения и системы управления базами данных.

Задание №11

Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

Выберите один из 4 вариантов ответа:

- 1) системой угроз;
- 2) системой защиты;
- 3) системой безопасности;
- 4) системой уничтожения.

Задание №12

К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

Запишите ответ:

Задание №13

Выделите группы, на которые делятся средства защиты информации:

Выберите один из 3 вариантов ответа:

- 1) физические, аппаратные, программные, криптографические, комбинированные;
- 2) химические, аппаратные, программные, криптографические, комбинированные;
- 3) физические, аппаратные, программные, этнографические, комбинированные;

Задание №14

По функциональному назначению средства инженерно-технической защиты делятся на следующие группы :

Продолжите ответ _____

Задание №15

Надежным средством отвода наведенных сигналов на землю служит

Запишите ответ:

Задание № 16

Установите соответствие

Укажите соответствие для всех 2 вариантов ответа:

1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи

2) наука скрывающая содержимое секретного сообщения

стеганография

криптография

Задание №17

Контроль доступа к информации обеспечивается последовательным использованием таких методов защиты информации...

Продолжите _____

Задание №18

Технический канал утечки информации...

Продолжите _____

Задание №19

Укажите соответствие для всех 4 вариантов ответа:

1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок

2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов

3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

защита информации от утечки по акустическому каналу

Защита информации от утечки по визуально-оптическому каналу

Защита информации от утечки по электромагнитным каналам

Защита информации от утечки по материально-вещественному каналу

Задание №20

Разновидности угроз безопасности

Выберите несколько из 6 вариантов ответа:

1) техническая разведка

2) программные

3) программно-математические

4) организационные

5) технические

6) физические

Итоговый тест МДК 03.02

Задание №1

Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

1. правовым методам защиты информации

2. организационно-техническим методам защиты информации
3. организационно-распорядительным методам защиты информации
4. экономическим методам защиты информации

Задание №2

Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

1. собственник информации
2. владелец информации
3. пользователь

Задание №3

Форма допуска, требуемая для работы со сведениями особой важности является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №4

Форма допуска, требуемая для работы с совершенно секретными сведениями является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №5

Форма допуска, требуемая для работы с секретными сведениями является:

1. первой формой допуска
2. второй формой допуска
3. третьей формой допуска

Задание №6

В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:

1. каждый пользователь допускаются должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
2. каждый пользователь допускаются должностными лицами только к информации, касающейся зоны его проживания
3. каждый пользователь допускаются должностными лицами ко всей информации, к которой у него есть форма допуска

Задание №7

Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:

1. незаконного оборота информации
2. взлома информации
3. несанкционированного использования информации

Задание №8

Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:

1. дезинформация
2. легендирование
3. шпионаж

Задание № 9

Какое направление защиты в основном применяется для охраны материальных ценностей?

1. инженерно-техническая
2. организационно-техническая
3. организационно-распорядительная
4. нормативно-правовая
5. экономическая

Задание №10

Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?

1. контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
2. инфракрасный светодиод лазерного принтера, посылающий кратковременные
3. вспышки на электризованную поверхность фоточувствительного барабана
4. модулированный по силе тока поток электронов, засвечивающий в определенном
5. порядке пиксели люминофора электронно-лучевой трубки
6. экран компьютерного монитора и глаза пользователя
7. оптический канал связи
8. все варианты могут быть отнесены к техническим каналам связи

Задание №11

Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №12

Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №13

Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №14

Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радицепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №16

Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

1. визуально-оптический канал
2. электромагнитный канал
3. виброакустический канал
4. материально-вещественный канал

Задание №17

Примером какого канала утечки информации служит звук голоса человека?

1. визуально-оптического канала
2. электромагнитного канала
3. виброакустического канала
4. материально-вещественного канала

Задание №18

По какому признаку делят на классы средства технической разведки (СТР) ?

1. по дальности канала
2. по форме допуска
3. по мощности
4. по степени финансирования

Задание №19

Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле относят к ...

1. первому классу СРТ
2. второму классу СРТ
3. третьему классу СРТ

Задание №20

Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ...

1. первого класса
2. второго класса
3. третьего класса

Вопросы для промежуточной аттестации

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства
4. Аппаратные средства
5. Программные средства
6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
8. Генераторы шума.
9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.
18. . Концепции инженерно-технической защиты информации.
19. Системный подход к защите информации.
20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.
22. Направления инженерно-технической защиты информации.
23. Показатели эффективности инженерно-технической защиты информации.
24. Теоретические основы инженерно-технической защиты информации.
25. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений.
27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта.
31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Распространение сигналов в технических каналах утечки информации.
35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты.
37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам.
40. Организационные основы инженерно-технической защиты информации.
41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.

44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации по оценке эффективности защиты информации.
46. Инженерно-техническая защита
47. Физические средства
48. Аппаратные средства
49. Программные средства
50. Криптографические средства
51. ПК на предмет определения максимального расстояния, при котором информацию можно снять с ПК, физически не подключаясь к нему;
52. Оценивается система видеонаблюдения помещения, где расположен сервер;
53. Проверяются помещения, предназначенные для переговоров, на предмет наличия различных подслушивающих устройств;
54. Производится установка специального оборудования, призванного распознавать подслушивающие устройства
55. Утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности
56. Детекторы, индикаторы поля и тест-приёмники;
57. Анализаторы проводных коммуникаций;
58. Многофункциональные поисковые приборы;
59. Обнаружители скрытых видеокамер;
60. Нелинейные локаторы;
61. Комплексы радиомониторинга и пеленгования;
62. Средства защиты от утечки акустической информации;
63. Устройства противодействия радиоэлектронным средствам негласной аудиозаписи;
64. Устройства блокирования работы систем проводной, мобильной связи и передачи данных;
65. Устройства защиты от прослушивания телефонных переговоров;
66. Устройства защиты от утечки информации по цепям электропитания (фильтры помехоподавляющие электрические) и заземления;
67. Устройства защиты от утечки информации по каналам ПЭМИН;
68. Устройства хранения, копирования, уничтожения и восстановления информации;
69. Цифровые системы регистрации, звукозаписи и шумоочистки речевых сигналов;
70. Металлодетекторы ручные досмотровые;
71. Металлоискатели поисковые грунтовые, глубинные;
72. Металлодетекторы арочные стационарные досмотровые;
73. Программных средств сбора, анализа и обработки информации;
74. Радиоэкранирующих и радиопоглощающих материалов шумопоглощающих материалов.
75. Комплексное использование технических, программных и организационных средств
76. Информация как объект защиты
77. Требования к защищенности информации
78. Организационные меры защиты информации
79. Оценка вероятного противника
80. Оценка условий решения задачи защиты информации
81. Инженерно-технические меры защиты информации
82. Системы информационной безопасности
83. Принципы построения систем безопасности
84. Защита компьютерной информации
85. Угрозы несанкционированного доступа в сеть
86. Системы информационной безопасности сети
87. Принципы построения систем безопасности сети
88. Аппаратные средства защиты передаваемых данных
89. Разработка системы управления объектом защиты и безопасности
90. Постановка задачи проектирования

91. Анализ объекта защиты
92. Контролируемая зона
93. Возможные каналы утечки информации
94. Разработка политики защиты контролируемой зоны
95. Обеспечение защиты помещения проведения совещаний
96. Обеспечение защиты помещения руководителя
97. Обеспечение защиты помещения серверной
98. Разработка политики безопасности сети и коммуникаций
99. Интернет-шлюз + фаерволл как основа системы управления
100. Выбор и конфигурирование аппаратных средств защиты данных
101. Защита данных средствами защиты информации и специального ПО
102. Описание настройки специального программного обеспечения защиты данных
103. Моделирование объектов защиты.

| ПАКЕТ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ | | |
|---|---|-----------------------------|
| Результаты (освоенные профессиональные компетенции) | Формы и методы контроля и оценки | Отметка о выполнении |
| ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях. | экспертная оценка выполнения практической работы | |
| ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях | экспертная оценка выполнения практической работы установке программного обеспечения | |
| ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями. | Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения | |
| ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей. | Наблюдение и экспертная оценка выполнения работ по обновлению и техническому сопровождению программного обеспечения | |

Список использованной литературы

Печатные издания:

1. Технические средства и методы защиты информации / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. 7-е изд., испр. - Москва :Гор. линия-Телеком , 2023. -616 с.
2. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва : Академия, 2022. - 336 с. (Специальности среднего профессионального образования). - URL: <https://academia-moscow.ru> - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный
3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2107178> (дата обращения: 28.03.2024)
4. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1912987> (дата обращения: 01.04.2024)
5. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с.— DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2082642> (дата обращения: 01.04.2024).
6. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2024. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://ezpro.fa.ru:2058/bcode/543873> (дата обращения: 01.04.2024)
7. Мельников, В. П., Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. — Москва : КноРус, 2023. — 371 с. — ISBN 978-5-406-11960-0. — URL: <https://book.ru/book/950148> (дата обращения: 01.04.2024)
8. Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2022. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1359091> (дата обращения: 01.04.2024).
9. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ИНФРА-М, 2022. — 256 с. - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1861659> (дата обращения: 01.04.2024).
10. Фомичев, В. М. Криптографические методы защиты информации (курс лекций) : учебное пособие / В. М. Фомичев. - Москва : Прометей, 2023. - 340 с. - ISBN 978-5-00172-538-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2124893> (дата обращения: 01.04.2024)

Электронные издания (электронные ресурсы):

11. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru.
12. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru.

13. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>.

14. Федеральный портал «Информационно-коммуникационные технологии в образовании» <http://www.ict.edu.ru>.

15. <http://www.morion.ru/>.

16. <http://www.nateks.ru/>.

17. <http://www.iskratel.com/>.

18. <http://www.ps-ufa.ru/>.

19. <http://3m.com/>.

20. <http://www.rusgates.ru/index/php> - Материалы сайта завода «Ферроприбор».

Дополнительные источники:

21. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

22. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

23. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

24. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

25. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

26. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

27. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

28. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

29. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

30. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

31. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

32. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

33. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

34. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

35. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
36. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
37. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
38. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
39. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
40. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
41. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
42. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
43. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.
44. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.
45. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.
46. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.
47. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью.
48. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
49. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
50. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

51. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи".
 52. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования".
 53. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
 54. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
 55. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
 56. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
 57. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
 58. Номенклатура показателей качества. Ростехрегулирование, 2005.
 59. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
 60. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
 61. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
 62. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
 63. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
 64. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
 65. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
 66. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
 67. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
 68. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
- Отечественные журналы:**
69. "InformationSecurity/ Информационная безопасность".
 70. Системный администратор.
 71. Компьютер ПРЕСС.

72. Системы безопасности. Журнал для руководителей и специалистов в области безопасности.

73. Сети и системы связи.

Интернет Ресурсы:

74. <http://cryptogrof.ru/>