МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине
Техническая защита информации
(наименование дисциплины)

10.05.02 Информационная безопасность телекоммуникационных систем, профиль «Защита информации в системах связи и управления»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Технические разведки. Общие сведения.

1. Элементы, содержащиеся в любой системе технической разведки.
2. Реализация обнаружения и анализа демаскирующих признаков в системе технической разведки.
3. Операции выполнения ДП по физической сути.
4. Прямые и побочные каналы утечки информации.
5. Специальные технические средства и решения, формирующие каналы утечки информации.
6. Достоинства и недостатки технической разведки.
7. Классификация технических разведок по видам носителей аппаратуры разведки.
8. Классификация технических разведок по способу добывания информации и типу аппаратуры разведки.
9. Что такое технические средства разведки?
10. Что является основным методом разведки?

Тема 2. Радиоэлектронная разведка.

1. Этапы разделение радиоэлектронной разведки.
2. Критерии выбора стратегий разведки и маскировки
3. Способы определения частоты сигналов РЭС.
4. Назовите основные способы пеленгации радиоэлектронных средств.
5. Принципы работы доплеровского пеленгатора.
6. Назначение радиолокационная разведка.
7. Сущность теплового радиоизлучения.
8. Разведка побочных электромагнитных излучений и наводок.
9. Задачи радиоэлектронной разведки
10. Цели радиоэлектронной разведки

Тема 3. Оптическая разведки.

1. Основные сведения об оптических линзовых системах.
2. Основные этапы визуально-оптическая разведка.
3. Фотографическая и фототелевизионная разведка.
4. Диагностические тепловые системы с охлаждаемыми и неохлаждаемыми приемниками излучения.
5. Назначение теплопеленгационной станции.
6. В чем заключается оптическая локация ?
7. Структурная схема дальномерного канала.
8. Задачи оптической разведки

9. Цели оптической разведки
10. Что необходимо определить при организации разведки?

Тема 4. Акустическая разведка.

1. Область применения параболического микрофона.
2. Акустические закладные устройства.
3. Использование закладных устройств.
4. Классификация радиозакладок по используемому диапазону.
5. Скрытая запись на диктофон как способ документирования информации.
6. Акустические закладки использующие телефонные линии.
7. Использование диапазона радиоволн.
8. Методы обработки речевых сигналов.
9. Назовите основные характеристики направленных микрофонов.
10. Использование адаптивного фильтра.

Тема 5. Компьютерная разведка.

1. Методы взлома компьютерных систем.
2. Программы шпионы.
3. Классификация программных закладок.
4. Основные группы деструктивных действий, осуществляемые программными закладками.
5. Модели воздействия программных закладок на компьютеры.
6. Статистическое и динамическое искажения.
7. Клавиатурные шпионы.
8. В чем заключается метод криптоаналитических закладок ?
9. Задачи компьютерной разведки
10. Цели компьютерной разведки

Тема 6. Средства технической разведки.

1. Сделайте выборку средств космической разведки.
2. Назовите основные средства воздушной разведки.
3. Какие средства контроля классификаций морская разведка бывают ?
4. Автоматические устройства технической разведки кабельных линий.
5. Портативная техника для разведслужб.
6. Скрыто устанавливаемые микрофоны.
7. Классификация радиопередатчиков телефонных линий.
8. Какие технические средства используется для ведения войсковой разведки?
9. Что такое технические средства разведки?
10. Что является основным методом разведки?

Тема 7. Противодействия техническим разведкам.

1. Роль противодействия техническим средствам разведки.
2. Этапы управления сложными системами.
3. Методы борьбы с системами и средствами управления противника.
4. Способы достижения противодействия распознаванию типа объекта.
5. Основные направления противодействия ТСР. Сравнение скрытия информации и технической дезинформации.
6. Кто регулирует деятельность в области защиты информации?
7. Каковы основные задачи Фстэк?
8. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?
9. Как осуществляется защита информации?
10. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?

Тема 8. Радиоэлектронная противодействие и радиомаскировка.

1. Назовите цель пассивной радиомаскировки.
2. Цель применения экранирования.
3. Основное назначение фильтров. Типы фильтров.
4. Требования к заземлению технических средств.
5. Что представляют собой специальные помещения и с какой целью они используются?
6. Способы маскировки от средств радиолокационной разведки.
7. Назовите цель активной радиомаскировки.
8. Перечислите способы активного подавления РЛС.
9. Какие особенности противодействия радио- и радиотехнической разведке?
10. Какие существуют методы криптографической защиты информации?

Тема 9. Противодействие акустической разведки.

1. В чём заключается метод слухового контроля? Цель его применения.
2. Какие существуют пассивные методы акустической защиты?
3. Эффективность применения экранных глушителей звука.
4. Характеристика прозрачных переговорных кабин.
5. Как осуществляется оценка звукоизоляции объекта?
6. Какие существуют активные методы акустической защиты?
7. Технические защитные устройства.
8. Какие демаскирующие признаки называются именными, чем они отличаются от других признаков?

9. Какие демаскирующие признаки называются прямыми, чем они отличаются от других признаков?

10. Какие демаскирующие признаки называются косвенными, чем они отличаются от других признаков?

Тема 10. Противодействие видовой разведки.

1. Как осуществляется защита от оптической и оптикоэлектронной разведок?

2. Назовите способы достижения нарушения контакта при противодействии средствам оптической и радиолокационной разведке (РЛР).

3. Что представляет собой защита от видовой РЛР?

4. Способы снижения уровня сигнала на входе приёмника РЛС.

5. Дайте определения понятиям модуляции и демодуляции сигналов. Опишите и нарисуйте, какие типы импульсно-манипулированных сигналов Вы знаете?

6. Какие типы и виды помех в каналах связи Вы знаете?

7. Классификация помех в каналах связи. Дайте определения мультипликативной и аддитивной помехам.

8. Какие виды носителей информации Вы знаете? Как осуществляется запись информации на носитель?

9. Перечислите основные источники функциональных сигналов.

10. Проведите классификацию источников опасных сигналов по их физическому происхождению.

Тема 11. Защита от внедряемых на объекты разведывательных устройств.

1. Этапы защиты от внедряемых на объекты разведывательных устройств.

2. Содержание поисковых мероприятий.

3. Назовите цель применения рентгеновского контроля.

4. Сравнительная характеристика поисковых приборов.

5. Основная задача обследования помещений.

6. Цель проведения проверки электроустановок и коммуникаций.

7. Принцип действия электромагнитных, электродинамических и магнитострикционных акустоэлектрических преобразователей.

8. Принцип действия емкостных акустоэлектрических преобразователей. Принцип действия пьезоэлектрических акустоэлектрических преобразователей.

9. Типы угроз, создаваемых акустоэлектрическими преобразователями.

10. Назовите источники побочных высокочастотных излучений. Назовите источники побочных низкочастотных излучений.

Тема 12. Технические средства защиты информации.

1. Область применения нелинейных локаторов.

2. Какие существуют методы защиты информации от утечки по электромагнитному каналу?

3. Предназначение отсекающего линейного фильтра.

4. Способ предотвращения несанкционированного использования сотовых телефонов.

5. Сравните отечественные и зарубежные помехоподавляющие фильтры.

6. Перечислите цели защиты информации. Перечислите задачи ТЗИ.

7. Какие признаки объекта защиты называют демаскирующими?

8. Приведите классификацию демаскирующих признаков объекта защиты.

9. Охарактеризуйте видовые демаскирующие признаки.

10. Охарактеризуйте демаскирующие признаки сигналов.

Критерии оценки:

4-3 балла (или оценка «отлично») выставляется обучающемуся, если ондемонстрирует глубокое знание содержания вопроса; дает точные определения основныхпонятий; аргументированно и логически стройно излагает учебный материал; иллюстрируетсвой ответ актуальными примерами (типовыми и нестандартными), в том числесамостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросахпреподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеетсодержанием вопроса, но допускает некоторые недочеты при ответе; допускаетнезначительные неточности при определении основных понятий; недостаточноаргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свойответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если оносвоил основные положения контролируемой темы, но недостаточно четко дает определениеосновных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа;нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если онне владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основныеопределения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе наних грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа №1 «Анализ технических средств перехвата информации в оптическом диапазоне»

1) Перечислите характеристики технического канала утечки информации.
2) Перечислите показатели, характеризующие оптический прибор перехвата.
3) Перечислите принципы выявления закладных устройств оптического перехвата.
4) Каковы основные способом борьбы с утечкой информации по оптическим каналам?
5) Какие мероприятия должны быть предусмотрены при построении системы защиты оптических каналов?
6) Перечислите характеристики средств наблюдения.
7) Какая информация может быть получена по оптическому каналу?
8) Что является носителем информации в оптическом канале утечки информации?
9) Что входит в технический канал утечки информации?
10) Какие существуют каналы утечки информации?

Лабораторная работа №2 «Анализ технических средств перехвата информации в радиоэлектронном и электромагнитном диапазонах»

1) Какие задачи выполняют органы радиотехнической разведки?
2) Из чего состоит типовой комплекс перехвата радиосигналов?
3) Что такое антенна?
4) Что такое радиоприёмник?
5) Функции радиоприёмника
6) Виды радиоприёмников
7) Что относится к техническим каналам утечки информации по структуре?
8) В каком случае реализуется угроза утечки информации?
9) Какие существуют каналы утечки информации?
10) В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?

Лабораторная работа №3 «Анализ технических средств перехвата информации в акустическом диапазоне»

1) Область применения параболического микрофона?
2) Перечислите акустические закладные устройства.
3) Перечислите акустические закладки использующие телефонные линии.
4) Перечислите методы обработки речевых сигналов.
5) Назовите основные характеристики направленных микрофонов.

6) Какие средства могут использоваться для защиты информации от утечки по акустическому каналу?

7) Какие параметры необходимо учитывать при описании среды распространения?

8) Какие средства могут использоваться для перехвата речевой информации?

9) В чем заключается отличие между каналом передачи и каналом утечки информации?

10) Какие скрытые каналы могут быть при передаче информации?

Лабораторная работа №4 «Анализ технических средств перехвата информации в каналах, образованных средствами вычислительной техники»

1) Что такое технические средства приема, обработки, хранения и передачи информации (ТСПИ)?

2) Перечислите технические каналы утечки информации, как они классифицируются в зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата?

3) Что такое ВТСС?

4) Что такое случайная антенна?

5) Что такое электромагнитные каналы утечки информации?

6) Что такое параметрические каналы утечки информации?

7) Каким путем может осуществляться перехват информации обрабатываемой техническими средствами?

8) Что относится к техническим каналам утечки информации по структуре?

9) Какие каналы утечки информации могут возникать при работе средств вычислительной техники?

10) Какие существуют технические каналы утечки информации обрабатываемой основными техническими средствами и системами?

Лабораторная работа №5 «Анализ технических средств перехвата информации в материально-вещественном канале утечки»

1) Особенность материально-вещественного канала утечки информации.

2) Основные источники информации в материально-вещественном канале.

3) Утечка какого вида информации возможна в материально-вещественном канале?

4) Приемники информации в материально-вещественном канале утечки информации

5) Средства обнаружения утечки информации о радиоактивных веществах.

6) Что должно включать в себя описание технического канала утечки информации?

7) В каком техническом канале утечки информации носителем информации является упругая акустическая волна?

8) Что входит в технический канал утечки информации?

9) В чем заключается отличие между каналом передачи и каналом утечки информации?

10) Какие скрытые каналы могут быть при передаче информации?

Лабораторная работа №6 «Моделирование объекта защиты»

1) Какой основной объект анализа объекта защиты?
2) Что необходимо для создания полной модели объекта защиты?
3) Какие бывают уровни конфиденциальности информации?
4) Какие объекты обычно указывают на планах этажей зданий?
5) Что определяет уровень конфиденциальности информации?
6) Какие существуют виды моделирования?
7) В чем состоит предназначение моделирования?
8) Сколько этапов в моделировании?
9) Какие существуют теории и методы для моделирования системы защиты информации?
10) В чем заключаются основные принципы моделирования?

Лабораторная работа №7 «Моделирование технических каналов утечки информации»

1) Назовитеэлементы, содержащиеся в любой системе технической разведки.
2) Назовитедостоинства и недостатки технической разведки.
3) Назовите прямые и побочные каналы утечки информации.
4) Назовите способы достижения противодействия распознаванию типа объекта.
5) Как осуществляется защита от оптической и оптикоэлектронной разведок?
6) Назовите методы борьбы с системами и средствами управления противника.
7) Назовите этапы защиты от внедряемых на объекты разведывательных устройств.
8) Назовите демаскирующие признаки сетевых акустических закладок.
9) Какие существуют пассивные методы акустической защиты?
10) Назовите способ предотвращения несанкционированного использования сотовых телефонов.

Критерии оценки:

6-5 баллов (или оценка «отлично») выставляется обучающемуся, если ондемонстрирует глубокое знание содержания вопроса; дает точные определения основныхпонятий; аргументированно и логически стройно излагает учебный материал; иллюстрируетсвой ответ актуальными примерами (типовыми и нестандартными), в том числесамостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросахпреподавателя.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеетсодержанием вопроса, но допускает некоторые недочеты при ответе; допускаетнезначительные неточности при определении основных понятий; недостаточноаргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свойответ типовыми примерами.

2-1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если оносвоил основные положения контролируемой темы, но недостаточно четко дает определениеосновных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа;нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если онне владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основныеопределения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе наних грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1) Перехват с применением оптической техники называется:

1. активный перехват
2. пассивный перехват
3. аудиоперехват
4. видеоперехват
5. просмотр мусора.

2) Перехват заключающийся в фиксации электромагнитных излучений, появляющихся при работе средств компьютерной техники называется:

1. активный перехват
2. пассивный перехват
3. аудиоперехват
4. видеоперехват
5. просмотр мусора.

3) Перехват с применением подслушивающего устройства в аппаратуру средств обработки информации называется:

1. активный перехват
2. пассивный перехват
3. аудиоперехват
4. видеоперехват
5. просмотр мусора.

4) Угроза безопасности информации вызванная естественно спровоцирована:

1. деятельностью человека
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
4. корыстными устремлениями злоумышленников
5. ошибками при действиях персонала.

5) Угрозы безопасности информации вызванная искусственно спровоцирована:

1. деятельностью человека
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
4. корыстными устремлениями злоумышленников
5. ошибками при действиях персонала.

6) К угрозам (случайным, искусственным) АСОИ относится:

1. физическое разрушение системы путем взрыва, поджога и т.п.
2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи
3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.
4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

7) Активный перехват информации это перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций
3. неправомерно использует технологические отходы информационного процесса
4. осуществляется путем использования оптической техники
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

8) … - Совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

(1) несанкционированный канал утечки информации

(2) технический канал утечки информации

(3) параметрический канал утечки информации

(4) физический канал утечки информации

9) Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена?

(1) угроза

(2) утечка

(3) уязвимость

(4) атака

10) Что является носителем информации в оптическом канале утечки информации?

(1) акустическая волна

(2) электрическое поле

(3) электромагнитное поле

(4) световая волна

11) К какому техническому каналу утечки информации относится несанкционированное распространение за пределы контролируемой зоны вещественных носителей с защищаемой информацией?

(1) оптический

(2) акустический

(3) материально-вещественный

(4) радиоэлектронный

12) В каком техническом канале утечки информации носителем является упругая акустическая волна?

(1) оптический

(2) акустический

(3) материально-вещественный

(4) радиоэлектронный

13) Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?

(1) электромагнитный

(2) электрический

(3) индукционный

14) Как называется технический канал утечки информации, заключающийся в перехвате электромагнитных излучений на частотах работы передатчиков систем и средств связи?

(1) электромагнитный

(2) электрический

(3) индукционный

15) Как называется технический канал утечки информации, при котором производится бесконтактный съем информации с кабельных линий связи?

(1) электромагнитный

(2) электрический

(3) индукционный

16) В каких технических каналах утечки акустической информации средой распространения информативного сигнала являются конструкции зданий, стены, потолки и другие твердые тела?

(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

17) В каких технических каналах утечки акустической информации основным средством съема информации является микрофон?

(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

18) В каких технических каналах утечки акустической информации основным средством съема информации является стетоскоп?

(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

19) В каких технических каналах утечки акустической информации основным средством съема информации является лазер?

(1) воздушные

(2) вибрационные

(3) электроакустические

(4) оптико-электронные

20) Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС под давлением звуковой волны может измениться взаимное расположение элементов схем, проводов и т.п.?

(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

21) Возникновение каких каналов утечки акустической информации обусловлено тем, что в ВТСС и ОТСС есть элементы, обладающие "микрофонным эффектом"?

(1) воздушные

(2) вибрационные

(3) электроакустические

(4) параметрические

22) Как называются электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях?

(1) вспомогательные электромагнитные излучения

(2) вторичные электромагнитные излучения

(3) побочные электромагнитные излучения

(4) недекларированные электромагнитные излучения

23) К какому типу технических каналов утечки относится перехват информации путем высокочастотного облучения технических средств?

(1) электромагнитные

(2) параметрические

(3) электрические

24) Какой тип технических каналов утечки образуется за счет просачивания информационных сигналов в цепи заземления и электропитания ОТСС?

(1) электромагнитные

(2) параметрические

(3) электрические

25) В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?

(1) оптический

(2) радиоэлектронный

(3) акустический

(4) материально-вещественный

26) В каком техническом канале утечки информации в качестве носителей используются фотоны?

(1) оптический

(2) радиоэлектронный

(3) акустический

(4) материально-вещественный

27) Информативность канала оценивается по:

(1) количеству информации, которую может передать канал

(2) ценности информации, которая передается каналом

(3) величине помех в канале

(4) величине затухания сигнала в канале

28) Каналы, в которых утечка информации носит случайный разовый характер, называются:

(1) постоянные

(2) периодические

(3) эпизодические

(4) неконтролируемые

29) Каналы, в которых утечка информации носит достаточно регулярный характер, называются:

(1) постоянные

(2) периодические

(3) эпизодические

30) Какой диапазон акустических волн соответствует звуковому диапазону?

(1) 1 – 20 Гц

(2) 1– 300 Гц

(3) 300 – 16000 Гц

(4) 16000 Гц - 4 МГц

31) Ультразвуковому диапазону соответствуют акустические волны:

(1) 1 – 20 Гц

(2) 1– 300 Гц

(3) 300 – 16000 Гц

(4) 16000 Гц - 4 МГц

32) Какой из приведенных ниже диапазонов называется высокочастотным радиодиапазоном?

(1) 30 – 300 кГц

(2) 300 кГц – 3МГц

(3) 3 – 30 МГц

(4) 30 – 300 МГц

33) Если частота сигнала равна 20 Гц, то его период:

(1) 0,01 с

(2) 0, 05 с

(3) 20 с

(4) 5 минут

34) Если минимальная частота сигнала 30 КГц, а максимальная – 300 КГц, то ширина спектра сигнала будет равна:

(1) 360

(2) 330

(3) 270

(4) 240

35) К основным показателям ТКУИ относятся:

(1) длина канала

(2) мощность

(3) ширина спектра

(4) относительная информативность

(5) пропускная способность

36) Пропускная способность канала зависит от:

(1) ширины полосы пропускания канала

(2) длины канала

(3) относительной информативности канала

(4) соотношения сигнал/шум

37) Что является средой распространения сигнала в виброакустическом канале утечки информации?

(1) твердые тела

(2) воздух

(3) вода

(4) телефонная линия

38) Какое средство чаще всего используется злоумышленником для снятия информации в виброакустическом канале утечки?

(1) микрофон

(2) лазер

(3) стетоскоп

(4) анализатор спектра

39) Какое средство используется злоумышленником для снятия информации с оптико-электронного канала утечки?

(1) микрофон

(2) лазер

(3) стетоскоп

(4) анализатор спектра

40) Как называются технические каналы утечки информации, которые образуются в результате того, что звуковая волна давит на элементы схем, проводов и т.п. в ВТСС и ОТСС, изменяя индуктивность и емкость?

(1) параметрические каналы

(2) оптико-электронные каналы

(3) пассивные каналы

(4) вибрационные каналы

41) Выделите средства разведки, которые не требуют физического проникновения злоумышленника в защищаемое помещение:

(1) стетоскопы

(2) диктофоны

(3) направленные микрофоны

(4) лазерные микрофоны

(5) радиозакладки

(6) проводниковые микрофоны

42) Выделите средства разведки, которые требуют физического проникновения злоумышленника в защищаемое помещение:

(1) стетоскопы

(2) диктофоны

(3) направленные микрофоны

(4) лазерные микрофоны

(5) радиозакладки

(6) проводниковые микрофоны

43) Как называется устройство разведки, которое передает информацию злоумышленнику с помощью электромагнитных волн радиочастотного диапазона?

(1) микрофон

(2) радиозакладка

(3) диктофон

(4) радиомаяк

(5) анализатор спектра

44) Выберите утверждения, верные для ИК-передатчиков:

(1) ИК-передатчики можно обнаружить с помощью приемника контроля

(2) ИК-передатчик нельзя обнаружить с помощью приемника контроля

(3) ИК-передатчики дешевле, чем обычные радиозакладки

(4) ИК-передатчики дороже, чем обычные радиозакладки

(5) ИК-передатчики потребляют мало энергии

(6) ИК-передатчики потребляют много энергии

45) По какому каналу передает информацию ИК-передатчик?

(1) оптический

(2) радиоэлектронный

(3) акустический

(4) линии электропитания

46) Как называются закладки, использующие для передачи информации силовые линии?

(1) ИК-передатчики

(2) стетоскопы

(3) сетевые закладки

(4) радиозакладки

47) Какое напряжение обычно используется для питания маленьких проводных микрофонов?

(1) 9-15 В

(2) 30-45 В

(3) 100-150В

(4) 220 В

48) Ослабление звука в параболическом микрофоне тем сильнее, чем:

(1) больше угол волны по отношению к оси

(2) меньше угол волны по отношению к оси

(3) чем больше диаметр микрофона

(4) чем меньше диаметр микрофона

49) Как называется микрофон, который принимает звук вдоль линии, совпадающей с направлением источника звука?

(1) параболические микрофоны

(2) плоские микрофоны

(3) трубчатые микрофоны

(4) проводные микрофоны

50) Как называется микрофон, представляющий из себя фазированную акустическую решетку, в узлах которой размещаются микрофоны?

(1) параболический микрофон

(2) плоский микрофон

(3) трубчатый микрофон

(4) проводной микрофон

51) Что располагается в узлах фазированной акустической решетки плоского микрофона?

(1) ИК-датчики

(2) датчики движения

(3) микрофоны

(4) транзисторы

52) Что может использовать злоумышленник, если он хочет снять информацию с оконного стекла, которое вибрирует под воздействием акустических волн внутри помещения?

(1) параболический микрофон

(2) плоский микрофон

(3) трубчатый микрофон

(4) лазерный микрофон

53) По какому каналу принимает информацию лазерный микрофон?

(1) оптический

(2) радиоэлектронный

(3) акустический

(4) линии электропитания

54) что может использовать злоумышленник, если он хочет снять информацию с оконного стекла, которое вибрирует под воздействием акустических волн внутри помещения?

(1) стетоскоп

(2) плоский микрофон

(3) трубчатый микрофон

(4) лазерный микрофон

55) Для чего применяется экранирование помещений и дополнительное заземление объектов защиты?

(1) для увеличения уровня побочных электромагнитных излучений

(2) для уменьшения уровня побочных электромагнитных излучений

(3) для обеспечения бесперебойного питания объектов защиты

(4) для исключения внедрения злоумышленников во внутренние сегменты сети

56) Какое требование к системе защиты информации предполагает организацию единого управления по обеспечению защиты информации?

(1) адекватность

(2) непрерывность

(3) централизованность

(4) универсальность

57) Какое требование к системе защиты информации предполагает то, что методы защиты должны обеспечивать возможность перекрытия канала утечки информации, независимо от его вида и места появления?

(1) адекватность

(2) непрерывность

(3) централизованность

(4) универсальность

58) Канал утечки информации представляет собой совокупность…

(1) Источник информации, угроза безопасности информации, аппаратура перехвата информации

(2) Источник информации, среда распространения информации, приемник информации

(3) Источник информации, условия возникновения утечки информации, факторы воздействия на информацию

(4) Источник информации, приемник информации, угроза безопасности информации

59) Что располагается в узлах фазированной акустической решетки плоского микрофона?

(1) ИК-датчики

(2) датчики движения

(3) микрофоны

(4) транзисторы

60) Какое экранирование наиболее эффективно на высоких частотах?

(1) электростатическое

(2) магнитостатическое

(3) электромагнитное

61) Выберите из нижеперечисленного каналы утечки информации без использования технических средств:

(1) Канал утечки информации, обусловленный наводками

(2) Непреднамеренный просмотр информации

(3) Непреднамеренное прослушивание информации

(4) Канал утечки информации, передаваемой по оптическим линиям связи

62) Вспомогательные технические средства и системы (ВТСС) это:

(1) Технические средства, предназначенные для передачи информации ограниченного доступа

(2) технические средства, устанавливаемые с целью защиты информации ограниченного доступа

(3) технические средства, не предназначенные для обработки информации, но размещенные в том же помещении, где и объект информатизации

(4) технические средства, размещаемые в защищаемом помещении и предназначенные для обработки акустической информации ограниченного доступа

63) Укажите способы распространения информации при ее утечке каналу, обусловленному наводками:

(1) Цепь электропитания

(2) Цепь заземления

(3) Информативное электромагнитное поле

(4) Воздушное пространство

64) Выберите из списка технические каналы утечки речевой информации:

(1) Специально внедренные в предметы интерьера защищаемого помещения программные средства негласного получения информации

(2) Акустоэлектрический канал утечки информации

(3) Несанкционированный доступ к информации

(4) Наводки на цепи электропитания

65) Как называются помещения, специально предназначенные для проведения конфиденциальных мероприятий?

(1) контролируемые помещения

(2) защищаемые помещения

(3) ограниченные помещения

(4) конфиденциальные помещения

66) Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации?

(1) субъект защиты

(2) автоматизированная система

(3) объект информатизации

(4) объект защиты

67) Выделите технические мероприятия с использованием пассивных средств защиты информации:

(1) звукоизоляция

(2) пространственное зашумление

(3) линейное зашумление

(4) заземление

(5) экранирование

68) Как называются технические средства защиты, которые уменьшают отношение сигнал/шум на входе аппаратуры злоумышленника?

(1) активные

(2) пассивные

(3) динамические

(4) статичные

69) Как называются технические средства защиты, которые ослабляют уровень информативного сигнала?

(1) активные

(2) пассивные

(3) динамические

(4) демаскирующие

70) Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений?

(1) административное

(2) техническое

(3) правовое

(4) организационное

71) Как называется мероприятие по защите информации, проведение которого не требует применения специально разработанных технических средств?

(1) административное

(2) техническое

(3) правовое

(4) организационное

72) Выделите организационные меры защиты информации от утечки по ТКУИ.

(1) определение границ контролируемой зоны

(2) экранирование ОТСС

(3) пространственное зашумление

(4) введение временных ограничений в режимах использования технических средств

73) Выделите технические мероприятия с использованием активных средств защиты информации:

(1) звукоизоляция

(2) пространственное зашумление

(3) линейное зашумление

(4) заземление

(5) экранирование

74) К какому типу мероприятий по защите информации относится уничтожение закладных устройств, подключенных к линии, с помощью специальных генераторов импульсов?

(1) организационные мероприятия

(2) технические мероприятия с использованием активных средств защиты

(3) техническое мероприятие с использованием пассивных средств защиты

75) Выделите верное утверждение. Напряженность электрического поля…

(1) прямо пропорциональна первой степени расстояния от источника сигнала

(2) прямо пропорциальна второй степени расстояния от источника сигнала

(3) обратно пропорциональна первой степени расстояния от источника сигнала

(4) обратно пропорциальна второй степени расстояния от источника сигнала

76) Какой тип экранирования заключается в замыкании электростатического поля на поверхность металлического экрана и отводе электрических зарядов на землю с помощью контура заземления?

(1) электростатическое

(2) магнитостатическое

(3) электромагнитное

77) Какое экранирование наиболее эффективно на высоких частотах?

(1) электростатическое

(2) магнитостатическое

(3) электромагнитное

78) Заземление состоит из:

(1) экрана

(2) заземлителя

(3) заземляющего проводника

(4) усилителя

79) Какие устройства применяются для фильтрации в цепях питания технических средств?

(1) радиочастотометры

(2) разделяющие трансформаторы

(3) интерсепторы

(4) помехоподавляющие фильтры

80) Как называется устройство, которое пропускает сигналы с частотами, лежащими в заданной полосе частот, и подавляет (ослаблять) сигналы с частотами, лежащими за пределами этой полосы?

(1) радиочастотометр

(2) разделяющий трансформатор

(3) интерсептор

(4) помехоподавляющий фильтр

81) Какое зашумление используется для исключения перехвата ПЭМИН по электромагнитному каналу?

(1) пространственное

(2) параллельное

(3) последовательное

(4) линейное

82) Какое зашумление используется для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС?

(1) пространственное

(2) параллельное

(3) последовательное

(4) линейное

83) Какой федеральный орган осуществляет деятельность по аккредитации объектов информатизации?

(1) ФСБ

(2) ФСТЭК

(3) Роспотребнадзор

(4) Минкомсвязь

84) Какая форма оценки соответствия используется для официального подтверждения эффективности используемых мер и средств по защите этой информации на конкретном объекте информатизации?

(1) аккредитация

(2) аттестация

(3) сертификация

(4) лицензирование

85) Как называется сигнал, который передает защищаемую информацию и может быть перехвачен злоумышленником с дальнейшим извлечением этой информации?

- информационный
- демаскирующий
- опасный
- функциональный

86) Как называются опасные сигналы, которые создаются техническим средством обработки информации для выполнения заданных функций?

- случайные
- намеренные
- функциональные
- демаскирующие

87) Как называются методы защиты акустической информации, предусматривающие подавление технических средств разведки?

- превентивные
- проактивные
- пассивные
- активные

88) Для подавления диктофонов используют генераторы мощных шумовых сигналов … диапазона частот.

- миллимитрового
- метрового
- сантиметрового
- дециметрового

89) Как называются акустоэлектрические преобразователи, в которых под воздействием акустической волны возникают эквивалентные электрические сигналы?

- активные
- электрические
- пассивные
- емкостные

90) Какой режим работы сканирующего приемника будет использовать потенциальный злоумышленник, если знает, на каких частотах работают интересующие его приборы?

- режим сканирования слепых зон
- режим автоматического сканирования по фиксированным частотам
- ручной режим работы
- режим автоматического сканирования в заданном диапазоне частот

91) Какой компонент комплекса для перехвата радиосигналов предназначен для определения параметров сигнала (частота, вид модуляции, структура кода и т.п.)?

- радиоприемник
- анализатор технических характеристик сигнала
- радиоперенгатор
- антенна
- регистрирующее устройство

92) Какие параметры электрических цепей чаще всего изменяются под воздействием акустической волны в пассивных акустоэлектрических преобразователях?

- индуктивность
- сопротивление
- длина
- емкость

93) Как называется паразитная связь, возникающая в результате воздействия магнитного поля?

- гальваническая
- емкостная
- индуктивная
- магнитострикционная

94) Как называется паразитная связь, возникающая в результате воздействия электрического поля?

- емкостная
- магнитострикционная
- гальваническая
- индуктивная

95) На какие две категории делятся акустоэлектрические преобразователи по физическим процессам, порождающим опасные сигналы?

- пассивные
- электрические
- акустические
- активные

96) Какое устройство позволяет принимать и анализировать структуру сигнала в широком диапазоне частот?

- сканирующий приемник
- анализатор спектра
- интерсептер
- радиотестер

97) Выберите правильные утверждения относительно переносимых и перевозимых сканирующих приемников:

- переносимые сканирующие приемники тяжелее перевозимых
- переносимые сканирующие приемники, как правило, менее функциональны, чем перевозимые
- переносимые сканирующие приемники, как правило, более функциональны, чем перевозимые
- переносимые сканирующие приемники легче перевозимых

98) Как называется способ защиты информации от утечки через ПЭМИН, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

- зашумление
- экранирование
- ослабление
- магнитострикция

99) Магнитная проницаемость материала экрана при магнитостатическом экранировании должна быть:

- как можно меньше
- не имеет значения
- как можно больше
- равна 3

100) Какие устройства обеспечивают развязку первичной и вторичной цепей по сигналам наводки?

- разделяющие трансформаторы
- интерсепторы
- радиочастотометры
- помехоподавляющие фильтры

101) Какая характеристика сканирующего приемника может привести к увеличению количества ложных срабатываний?

- скорость сканирования
- количество каналов
- габариты
- чувствительность

102) В основу работы какого устройства контроля положено изменение плотности среды вокруг радиозакладки?

- тепловизор
- металлодетектор
- анализатор спектра
- радиочастотометр

Задания в открытой форме

1. Перехват акустических сигналов по виброакустическим техническимканалам осуществляется …….

2. Оптико-электронный технический канал утечки информации образуется путем……..

3. Техническими средствами приёма, обработки и хранения информации являются……...

4. Дальняя зона электромагнитного поля располагается в границах……

5. Конфиденциальностью информации называется……

6. К коммерческой тайне относится информация……

7. Информационной безопасностью предприятия является……

8. В состав системы защиты информации входят обеспечивающие подсистемы……

9. Под угрозой безопасности информации понимается……

10. Причинами информационных угроз являются……

11. Основные компьютерные вирусы……

12. К основным законам информационной безопасности РФ относятся законы……

13. Основными принципами политики безопасности являются……

14. Политика безопасности верхнего уровня включает……

15. Удаленный доступ к сервису организован……

16. Политика управления паролями включает……

17. Системный подход к защите информации базируется на принципах……

18. Для ИБ используются программные средства……

19. Метод принуждения от метода побуждения отличается……

20. Криптография занимается……

21. Электронная подпись используется для……

22. В состав организационно-технических мер входит……

23. Межсетевые экраны применяют для……

24. Технические средства противодействия классифицируются……

25. В состав службы безопасности входят подразделения……

26. К мерам по защите информации в интернете относятся……

27. Межсетевые экраны-брандмауэры используются для……

28. Для защиты электронной почты используется……

29. Для защиты от вирусов можно использовать……

30. К антивирусным программам относятся……

31. Основные источники проникновения вирусов……

32. В корпоративной сети необходимо защищать……

33. Основные этапы построения системы защиты……

34. План защиты включает……

35. Ответственным за определение уровня классификации информации является……

36. Ответственность за гарантии того, что данные классифицированы и защищены несёт……

37. Политики безопасности – это……

38. Естественные угрозы безопасности информации вызваны……

39. Искусственные угрозы безопасности информации вызваны……

40. К посторонним лицам - нарушителям информационной безопасности относятся……

41. К основным непреднамеренным искусственным угрозам автоматизированным систем обработки информации относятся……

42. К внутренним нарушителям информационной безопасности относится……

Задания на установление соответствия

1. Установить соответствие между элементами и функциями

1	Подавление емкостных паразитных связей	А	Средства выявления каналов утечки информации
2	Телевизионные системы	Б	Защита информации от утечки по техническим каналам
3	Нелинейные локаторы	В	Аттестация объектов информатизации
		Г	Средства инженерной защиты объектов

2. Установить соответствие между способами и видами информации

1	По способу кодирования	А	Цифровая, аналоговая
2	По способу представления	Б	Визуальная, звуковая, документ
3	По способу обработки	В	Текстовая, графическая, числовая
		Г	Непрерывная, дискретная

3. Установить соответствие названия протокола его назначению

1	FTP	А	Протокол передачи данных
2	SMTP	Б	Протокол передачи файлов
3	TCP/IP	В	Протокол передачи гипертекста
		Г	Протокол передачи почты

4. Установить соответствие оборудования его назначению

1	Репитер	А	Устройство для объединения ПК в сетях Ethernet
2	Концентратор	Б	Устройство для высокоскоростной коммутации пакетов между портами
3	Коммутатор	В	Устройство для подключения и соединения нескольких локальных сетей
		Г	Повторитель, усилитель сигналов

5. Установить соответствие между каналами связи

1	Электромагнитные каналы	А	модулированные информационным сигналом (прослушивание радиотелефонов, сотовых телефонов, радиорелейных

			линий связи)
2	Электрические каналы	Б	подключение к линиям связи
3	Индукционный канал	В	эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов
		Г	емкостные, индуктивные и резистивные связи и наводки близко расположенных друг от друга линий передачи информации

6.Установить соответствие между элементами и функциями

1	Доступность	А	это критерий, который учитывает, насколько удобно источнику угроз использовать определенный вид уязвимости, чтобы нарушить информационную безопасность
2	Фатальность	Б	характеристика, которая оценивает глубину влияния уязвимости на возможности программистов справиться с последствиями созданной угрозы для информационных систем
3	Количество	В	характеристика подсчета деталей системы хранения и реализации информации, которым присущ любой вид уязвимости в системе.
		Г	насколько широко используется уязвимость в различных системах или приложениях.

7. Установить соответствие между видами технических каналов утечки информации

1	объекты или источники сигнала	А	работающее оборудования, документы, человек и его голос
2	среда распространения	Б	воздух, строительные конструкции, провода сети 220 В
3	закладное устройства	В	Прослушки , жучки , маячки
		Г	Компьютер, мобильный телефон, телевизор

8. Установите соответствие

1	NIST SP 800-39	А	предлагает для обеспечения безопасности и конфиденциальности использовать подход управления жизненным циклом систем
2	NIST SP 800-37	Б	предлагает трехуровневый подход к управлению рисками: организация, бизнес-процессы, информационные системы. Данный стандарт описывает методологию процесса управления рисками: определение, оценка, реагирование и мониторинг рисков
3	NIST SP 800-30	В	описывает подход к процессу мониторинга информационных систем и ИТ-сред в целях контроля примененных мер обработки рисков ИБ и необходимости их пересмотра
		Г	сфокусирован на ИТ, ИБ и операционных рисках, описывает подход к процессам подготовки и проведения оценки рисков, коммуницирования результатов оценки, а также дальнейшей поддержки процесса оценки

9. Установить соответствие между элементами и функциями

1	оптический канал	А	видовая информация — документы, изображения на мониторе, оборудование, новые модные коллекции, все, что можно увидеть или сфотографировать
2	модифицированный оптический канал	Б	оптико-электронный канал утечки речевой информации. Перехват ведется при помощи лазерного луча, испускаемого от лазерных акустических систем разведки (ЛАСР), а также триппель-призм (промежуточных

			элементов конструкции систем разведки, отражающих лазерный луч под определенным углом) на расстоянии до 500 метров
3	акустический канал	В	речь в помещении или из телефонного разговора. Мощный направленный микрофон перехватит сигнал на расстоянии до 100—150 м
		Г	перехватываются и преобразуются в данные колебания твердых сред — стекол, труб, строительных конструкций, вызываемые механическим воздействием звуковых волн

10. Установите соответствие между международной организации по стандартизации ISO

1	ISO/IEC 27005:2018	А	предлагает подходы к оценке необходимости приобретения киберстраховки как меры обработки рисков, а также к оценке и взаимодействию со страховщиком
2	ISO/IEC 27102:2019	Б	входит в серию стандартов ISO 27000 и является логически взаимосвязанным с другими стандартами по ИБ из этой серии. Данный стандарт отличается фокусом на ИБ при рассмотрении процессов управления рисками
3	ISO/IEC 31000:2018	В	описывает подход к риск-менеджменту без привязки к ИТ/ИБ. Методы оценки риска» ссылается 607-П ЦБ РФ «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков»

		Г	стандарт, разработанный для российских организаций, описывает процесс оценки рисков ИБ и рекомендации по управлению ими.

11. Установить соответствие между терминами и определениями

1	Объект защиты	А	информация, носители информации, технические средства и технология их обработки, а также средства защиты информации
2	Объект информатизации	Б	совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены
3	Защищаемые помещения (ЗП)	В	помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)
		Г	неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

12. Установить соответствие классификации угроз

1	Состояние источника угрозы	А	в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС;

			в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных
2	Степень влияния	Б	активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность, например, использование вредоносных вирусов или троянов; пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.
3	Возможность доступа сотрудников к системе программ или ресурсов		вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного); вред наносится после согласия доступа к ресурсам системы.
		Г	применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы; использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя.

13. Установить соответствие угроз безопасности информации в локальных размерах

1	Компьютерные вирусы	А	нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в основном они действуют локально;
2	«Черви»	Б	модификация вирусных программ, приводящая информационную систему в состояние блокировки и перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка каналов памяти и связи
3	«Троянские кони»	В	программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию
		Г	это тип вредоносных программ, которые могут скрыть свою активность и местоположение на компьютере, обходя стандартные методы обнаружения.

14. Установить соответствие между терминами и определениями

1	Автоматизированная система (АС)	А	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функции
2	Контролируемая зона (КЗ)	Б	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и

			посетителей организации, а также транспортных, технических и иных материальных средств
3	Специальные исследования (СИ)	В	выявление с использованием контрольно-измерительной аппаратуры возможных каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем
		Г	проверка технических средств и систем объекта защиты с целью выявления возможно внедренных электронных устройств съема информации (закладочных устройств)

15. Установить соответствие

1	Перехват паролей	А	мошенничество возможно с участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы.
2	«Маскарад»	Б	действия в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе -передача ложных данных в системе от имени другого человека
3	Незаконное использование привилегий	В	название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя
		Г	Кто-то получает доступ к конфиденциальной информации, не имея на это права, например, изучая чужие электронные письма

			или угнанный компьютер.

16. Установить соответствие между излучениями каналов

1	Побочные электромагнитные излучения и наводки (ПЭМИН)	А	паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники. В зависимости от среды распространения различают
2	Побочные электромагнитные излучения (ПЭМИ)	Б	нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации
3	Информативными ПЭМИ	В	сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением, выводимым на экран монитора, данными, обрабатываемыми на устройствах ввода-вывода и т.д.)
		Г	сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ

17. Установить соответствие между основными принципы защиты информации

1	Принцип законности	А	необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации
2	Принцип защиты информации	Б	основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных

			этапах решения задач сохранения секретов
3	Принцип приоритета	В	объектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
		Г	право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

18. Установить соответствие между терминами и определениями

1	Специальные обследования помещений	А	комплекс мер в области защиты информации в части проведения работ по выявлению электронных устройств, предназначенных для негласного получения сведений в помещениях, где циркулирует информация ограниченного пользования
2	Аттестация объекта защиты	Б	официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований РД по ЗИ
3	Основные технические средства и системы	В	технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации
		Г	установление нормативными документами численных значений показателей защищенности информации

19. Установить соответствие между элементами и функциями

1	Дробление	А	знание какой-то одной части информации не позволяет восстановить всю технологию в

			целом
2	Шифрование	Б	метод защиты информации сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от традиционных угроз
3	Кодирование	В	метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи
		Г	метод защиты информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником

20. Установить соответствие

1	Случайные антенны	А	вспомогательные технические средства, их соединительные линии, а также линии электропитания, посторонние проводники и цепи заземления, при непосредственном подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов
2	Сосредоточенные	Б	телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т. д., подключенные к линии, выходящей за пределы КЗ
3	Распределенные	В	кабели, провода, металлические

			трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ
		Г	телефонный аппарат, кабели также линии электропитания

Задания на установление правильной последовательности

1. Установить этапы разработки программного обеспечения:
1. Разработка алгоритма
2. Написание программы
3. Постановка задачи
4. Разработка математической модели

2. Установить этапы защиты от угроз безопасности:
1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам
2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet
3. Защита внешних каналов передачи информации
4. Разработка политики информационной безопасности
5. Анализ угрозы безопасности

3. Установить этапы стадии исполнения компьютерных вирусов:
1. Выполнение деструктивных функций
2. Передача управления программе-носителю вируса
3. Поиск жертвы
4. Заражение найденной жертвы
4. Загрузка вируса в память

4. Установить этапы построения системы антивирусной защиты сети:
1. Реализация плана антивирусной безопасности
2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности
3. Разработка политики антивирусной безопасности
4. Разработка плана обеспечения антивирусной безопасности

5. Установить этапы разработки модели:
1. Построение модели
2. Объект
3. Корректировка модели
4. Анализ результатов
5. Исследование модели на компьютере

6. Установить этапы построения программы обеспечения безопасности:

1. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности

2. Регулярный контроль пошаговой реализации плана безопасности

3. Установление уровня безопасности

4. Формирование политики безопасности организации

5. Определение ценности технологических и информационных активов организации

7. Установить действия этапа анализа рисков:

1. Оценка вероятности того, что угроза будет реализована на практике

2. Оценка рисков технологических и информационных активов

3. Идентификация и оценка стоимости технологических и информационных активов

4. Анализ угроз, для которых технологические и информационные активыявляются целевым объектом

8. Установить последовательность процессов для обнаружения и выдачи сигнала тревоги:

1. Одно системное событие не является неизбежно достаточным, чтобы утверждать, что это опасность

2. Если результат этой совокупности превышает пороговую величину, выдается сигнал тревоги

3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной

4. Каждое нарушение безопасности должно генерировать системное событие

9. Расположить параметры для группировки данных на сервере сбора информации об атаке:

1. Дата, время

2. Протокол

3. Порт получателя

4. Номер агента

5. IP-адрес атакующего

6. Тип атаки

10. Расположить в порядке возрастания даты разработки стандартов информационной безопасности:

1. ISO 27001:2005

2. ISO/IEC 17799

3. ISO/IEC 15408

4. «Критерии оценки доверенных компьютерных систем»

11. Расположить этапы процесса управления рисками информационной безопасности:

1. Классификация рисков, выбор методологии оценки рисков и проведение оценки

2. Анализ угроз и их последствий, определение слабостей в защите

3. Выбор, реализация и проверка защитных мер

4. Оценка остаточного риска

5. Идентификация активов и ценности ресурсов, нуждающихся в защите

6. Выбор анализируемых объектов и степени детальности их рассмотрения

12. Расположить этапы проведения аудита информационной безопасности:

1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы

2. Анализ полученных данных

3. Сбор исходных данных

4. Разработка регламента проведения аудита

14. Расположите в правильном порядке объекты защиты

1. __класс. Ценность данных определяется их собственником (коммерческая тайна)

2. __класс. Данные имеют ограниченный доступ на основании федеральных законов (персональные данные, банковская тайна)

3. __класс — государственная тайна.

Информационные объекты, имеющие ценность, присутствуют в жизни организации в виде

15. Расположить этапы процесса комплекса превентивных мер

1.подача и рассмотрение заявки;

2. предварительное ознакомление специалистов с аттестуемыми объектами;

3.разработка программы и методики испытаний;

4. запрос и получение специалистами необходимой технической документации;

5. проведение испытаний;

6. оформление, регистрация и выдача аттестата (сертификата соответствия) на оборудование и помещения.

16. Восстановите алгоритм испытаний

1. анализ информационных потоков, информационной системы в целом и отдельных объектов, технических средств, программного обеспечения, технической документации на внедренную систему защиты ИС в целом и от утечек по техническим каналам (ТКУИ);

2.оценка правильности классификации информационных объектов, выбора и применения технических средств защиты для блокирования опасных ТКУИ, возможных угроз несанкционированного доступа к информации и специальных воздействий на информацию (носители);

3. проверка сертификатов на программное обеспечение и техническое оборудование для защиты информации;

4. проведение аттестационных испытаний и оформление протоколов;

5.оформление заключения по результатам проверок.

17. Расположите этапы применения фреймворка управления рисками (NIST SP 800-37)

1. оценка внедренных мер защиты для определения корректности их применения, работоспособности и продуцирования ими результатов, удовлетворяющих требованиям безопасности и конфиденциальности

2. подготовка, т.е. определение целей и их приоритизация с точки зрения организации и ИТ-систем

3. внедрение мер защиты и описание того, как именно применяются меры защиты

4. категоризация систем и информации на основе анализа возможного негативного влияния от потери информации

5. выбор базового набора мер защиты и их уточнение (адаптация) для снижения риска до приемлемого уровня на основе оценки риска

6. непрерывный мониторинг систем и примененных мер защиты для оценки эффективности примененных мер, документирования изменений, проведения оценки рисков и анализа негативного влияния, создания отчетности по состоянию безопасности и конфиденциальности.

7. формальное согласование/утверждение использования систем или мер защиты на основе заключения о приемлемости рисков

18. Установить этапы реализации в ОС механизмов безопасности в порядке их внедрения:

1. Создание кольцевой системы защиты процессора

2. Реализация аутентификации пользователя

3. Реализация многозадачности

4. Создание виртуальных контейнеров для запуска приложений

19. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:

1. Опытная и промышленная эксплуатация
2. Проектный этап
3. Аттестация или декларирование
4. Предпроектный этап

20. Выберите правильную последовательность этапов разработки профиля защиты.

1. Анализ среды применения ИТ-продукта с точки зрения
2. безопасности.
3. Выбор профиля-прототипа.
4. Синтез требований.

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

В компании X используются компьютеры с USB-портами. Чтобы предотвратить возможность несанкционированной передачи данных, необходимо ограничить доступ к USB-портам. Какие меры безопасности можно применить для защиты USB-портов от утечки информации?

Компетентностно-ориентированная задача № 2

Разработать программу проведения аудита первой стороны, включающую:

- внутренние требования системы управления информационной безопасностью;
- состав проверяемых подразделений;
- вид аудиторской проверки;
- метрики оценки эффективности аудита

Компетентностно-ориентированная задача № 3

Разработать модель реализации преднамеренного инцидента информационной безопасности, с учетом:

- перечня злоумышленников;
- целей злоумышленников;
- методов и средств реализации информационного воздействия;
- действий злоумышленников;
- объектов информационного воздействия;
- результатов информационного воздействия.

Компетентностно-ориентированная задача № 4

В офисе компании обнаружены неизвестные беспроводные сети. Какие меры безопасности можно предпринять для защиты информации от возможной утечки через эти сети?

Компетентностно-ориентированная задача № 5

В организации А требуется ограничить физический доступ к помещениям с компьютерами, чтобы предотвратить утечку информации. Какие методы контроля доступа можно использовать для обеспечения безопасности?

Компетентностно-ориентированная задача № 6

В компании B регулярно происходят случаи несанкционированной передачи информации через технические каналы. Какие обучающие программы или мероприятия можно провести для повышения осведомленности сотрудников о безопасности информации и предотвращения утечек?

Компетентностно-ориентированная задача № 7

В компании C необходимо защитить передаваемую по сети информацию от возможных утечек. Какие алгоритмы шифрования можно использовать для обеспечения конфиденциальности данных и предотвращения утечек?

Компетентностно-ориентированная задача № 8

В компании D возникли подозрения на утечку информации через сетевой трафик. Какие инструменты и методы можно использовать для мониторинга и обнаружения несанкционированной передачи данных через технические каналы?

Компетентностно-ориентированная задача № 9

В организации E хотят обнаружить возможные скрытые устройства, которые могут использоваться для утечки информации. Какие методы и технологии можно применить для обнаружения таких устройств?

Компетентностно-ориентированная задача № 10

Компания F хочет улучшить физическую безопасность своих помещений для предотвращения утечки информации. Какие простые меры безопасности можно предложить, такие как установка замков, видеонаблюдение или контроль доступа?

Компетентностно-ориентированная задача № 11

В компании G пользователи часто становятся жертвами социальной инженерии и несанкционированной передачи информации. Какие тренинги или программы обучения можно провести, чтобы обучить пользователей распознавать и предотвращать утечку информации через технические каналы?

Компетентностно-ориентированная задача № 12

Компания H хочет проверить свою сеть на уязвимости, которые могут привести к утечке информации. Какие инструменты и методы можно использовать для сканирования сети и обнаружения потенциальных уязвимостей?

Компетентностно-ориентированная задача № 13

Компания I хочет обеспечить целостность своих данных и предотвратить возможные утечки информации. Какие методы и механизмы можно использовать для проверки целостности данных и обнаружения несанкционированных изменений?

Компетентностно-ориентированная задача № 14

В организации J необходимо управлять доступом к конфиденциальной информации и предотвращать ее утечку. Какие политики и процедуры можно внедрить для контроля доступа к данным и минимизации риска утечки через технические каналы?

Компетентностно-ориентированная задача № 15

В компании K возникли случаи использования несанкционированных устройств, которые могут быть потенциальным источником утечки информации. Какие методы и системы можно применить для обнаружения и блокирования подобных устройств?

Компетентностно-ориентированная задача № 16

В компании L широко используется электронная почта для обмена конфиденциальной информацией. Какие методы и средства шифрования можно применить для защиты электронной почты от возможных утечек и несанкционированного доступа?

Компетентностно-ориентированная задача № 17

Компания M хочет усилить безопасность своей сети и предотвратить утечку информации через компрометированные учетные записи. Какие методы и механизмы можно использовать для управления учетными записями и обнаружения несанкционированного доступа?

Компетентностно-ориентированная задача № 18

Компания N хочет обеспечить защиту своей сети от возможных вторжений и предотвратить утечку конфиденциальной информации. Какие методы и системы можно применить для обнаружения вторжений и минимизации риска утечки через технические каналы?

Компетентностно-ориентированная задача № 19

В организации O требуется непрерывный мониторинг сетевого трафика для обнаружения несанкционированных попыток доступа к конфиденциальной информации. Какие инструменты и технологии можно использовать для мониторинга сетевого трафика и обнаружения утечек?

Компетентностно-ориентированная задача № 20

В компании P часто происходит передача конфиденциальной информации через открытые каналы связи, что может привести к ее утечке. Какие методы и технологии можно использовать для обеспечения безопасной передачи информации через защищенные каналы связи?

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.