


Утверждаю  
Зам. директора по УР  
« 31 » 08 2023г.

 Иваненко И.В.

Согласовано  
Ведущий специалист-эксперт отдела по  
защите информации ГУ-ОПФ по Смо-  
ленской области  
« 31 » 08 2023г.

 Ефремов А.А.

Контрольно-оценочные материалы для промежуточной аттестации  
по МДК 03.01 Защита информации в информационно-телекоммуникационных системах и сетях с  
использованием технических средств защиты – 6 семестр  
для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных  
систем

Промежуточная аттестация по МДК 03.01 Защита информации в информационно-  
телекоммуникационных системах и сетях с использованием технических средств защиты, которая  
проходит в 6 семестре является другой формой аттестации в виде тестирования.

Профессиональные компетенции:

ПК 3.1	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях
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.
ПК 3.4	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Общие компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

Тест содержит 10 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блока (состоящих первый блок 30 вопросов, второй блок 20 вопросов) заданий по 5 вопросов. Время тестирования – 45 минут для каждой подгруппы (по 3 минуты на каждый вопрос из первого блока, по 6 минут на каждый вопрос закрытого типа).

Критерии оценивания

«5 баллов» - получают студенты, справившиеся с работой 100-90%;

«4 балла» - ставится в том случае, если верные ответы составляют 89-76% от общего количества;

«3 балла» - соответствует работа, содержащая 60-75% правильных ответов;

«2 балла» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
5 «отлично»	Студент набрал 5 баллов
4 «хорошо»	Студент набрал 4 балла
3 «удовлетворительно»	Студент набрал 3 балла
2 «неудовлетворительно»	Студент набрал 0-2 балла

## Первый блок

Формируемые ОК01, ОК 02, ОК 09, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4

1. Кто является основным ответственным за определение уровня классификации информации?
  - A. Руководитель среднего звена
  - B. Высшее руководство
  - C. Владелец
  - D. Пользователь
2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
  - A. Сотрудники
  - B. Хакеры
  - C. Атакующие
  - D. Контрагенты (лица, работающие по договору)
3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
  - A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
  - B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
  - C. Улучшить контроль за безопасностью этой информации
  - D. Снизить уровень классификации этой информации
4. Что самое главное должно продумать руководство при классификации данных?
  - A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
  - B. Необходимый уровень доступности, целостности и конфиденциальности
  - C. Оценить уровень риска и отменить контрмеры
  - D. Управление доступом, которое должно защищать данные
5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
  - A. Владельцы данных
  - B. Пользователи
  - C. Администраторы
  - D. Руководство
6. Что такое процедура?
  - A. Правила использования программного и аппаратного обеспечения в компании
  - B. Пошаговая инструкция по выполнению задачи
  - C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
  - D. Обязательные действия
7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
  - A. Поддержка высшего руководства
  - B. Эффективные защитные меры и методы их внедрения
  - C. Актуальные и адекватные политики и процедуры безопасности
  - D. Проведение тренингов по безопасности для всех сотрудников
8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
  - A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
  - B. Когда риски не могут быть приняты во внимание по политическим соображениям
  - C. Когда необходимые защитные меры слишком сложны
  - D. Когда стоимость контрмер превышает ценность актива и потенциальные потери
9. Что такое политики безопасности?
  - A. Пошаговые инструкции по выполнению задач безопасности
  - B. Общие руководящие требования по достижению определенного уровня безопасности
  - C. Широкие, высокоуровневые заявления руководства
  - D. Детализированные документы по обработке инцидентов безопасности
10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- A. Анализ рисков
  - B. Анализ затрат / выгоды
  - C. Результаты ALE
  - D. Выявление уязвимостей и угроз, являющихся причиной риска
11. Что лучше всего описывает цель расчета ALE?
- A. Количественно оценить уровень безопасности среды
  - B. Оценить возможные потери для каждой контрмеры
  - C. Количественно оценить затраты / выгоды
  - D. Оценить потенциальные потери от угрозы в год
12. Что такое тактическое планирование?
- A. Среднесрочное планирование
  - B. Долгосрочное планирование
  - C. Ежедневное планирование
  - D. Планирование на 6 месяцев
13. Что является определением воздействия (exposure) на безопасность?
- A. Нечто, приводящее к ущербу от угрозы
  - B. Любая потенциальная опасность для информации или систем
  - C. Любой недостаток или отсутствие информационной безопасности
  - D. Потенциальные потери от угрозы
14. Эффективная программа безопасности требует сбалансированного применения чего?
- A. Технических и нетехнических методов
  - B. Контрмер и защитных механизмов
  - C. Физической безопасности и технических средств защиты
  - D. Процедур безопасности и шифрования
15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют что?
- A. Внедрение управления механизмами безопасности
  - B. Классификацию данных после внедрения механизмов безопасности
  - C. Уровень доверия, обеспечиваемый механизмом безопасности
  - D. Соотношение затрат / выгод
16. Как расшифровывается аббревиатура СКУД?
- A. Система контроля и управления доступом;
  - B. Система катализации и управления доступом;
  - C. Система карт и управления доступом;
  - D. Система КПП и удержания диверсантов.
- 17.. СКУД по среднему количеству емкости точек доступа обычно, что содержит?
- A. от 32 до 64 точек доступа;
  - B. от 16 до 64 точек доступа;
  - C. от 50 до 100 точек доступа;
  - D. от 100 до 300 точек доступа.
18. С чем СКУД обычно интегрируется?
- A. С системой видеонаблюдения и системой охранно-пожарной сигнализации; +
  - B. С системой вентиляции на предприятии;
  - C. С системой охранной;
  - D. С системой пожарной.
19. Какое устройство, нельзя назвать преграждающим управляемым (УПУ)?
- A. Проходные шлюзы;
  - B. Проходные кабины;
  - C. Откатные ворота;
  - D. Дверь с навесным замком;
  - E. Шлагбаум.
20. Если СКУД идентифицируется по карточке и отпечатку пальца, то как он классифицируется?
- A. Многоуровневый;
  - B. Двухступенчатый.
  - C. Одноуровневый
  - D. Одноступенчатый

21. Какое главное отличие автономных СКУД от сетевых (централизованных)?
- А. Автономные могут функционировать без центрального пульта охраны;
  - Б. Количество точек на предприятии;
  - В. Сетевой может обходиться без блока питания.
22. К каким УПУ относится кабина проходная?
- А. частичным перекрытием;
  - Б. с полным перекрытием;
  - В. с блокированием объекта в проеме.
23. Что такое идентификация?
- 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.
24. Что такое аутентификация?
- 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).
25. Что такое УВИП?
- А. Устройства ввода идентификационных признаков;
  - Б. Упорядоченный ввод идентификационных признаков;
  - В. Устройства ввода идентификационных персон.
26. К достоинствам УВИП на базе идентификаторов Touch Memory что 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).
27. 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.
28. Какой электронный прибор называют металлоискатель (металлодетектор)?
- 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;
29. На чем основан принцип работы металлодетекторов?
- 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).
30. Какое главное преимущество арочного металлодетектора перед ручным?
- А. Высокая пропускная способность;
  - Б. Низкая вероятность ложной тревоги;
  - В. Компактность;
  - Г. Простота использования.

## Второй блок

Формируемые ОК01, ОК 02, ОК 09, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4

1. Что такое технический контроль (ТК)?
2. Что такое неразрушающий контроль (НК)?
3. Что такое техническая диагностика (ТД)?
4. В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации по каналам ПЭМИН можно разделить на какие виды?
5. Что относится к электромагнитным каналам утечки информации?
6. В ТСПИ Что является носителем информации в ТСПИ?
7. Что такое технический канал утечки информации (ТКУИ)?
8. В полосе частот от 200 Гц до 30 МГц в комплект антенн, что должно входить?
9. Под информацией понимают какие сведения?
10. Утечка информации - это процесс, какого вида, переноса конфиденциальной информации (КИ) от источника КИ к любому возможному получателю на любом этапе ее существования, включая нахождение в инфокоммуникационной системе?
11. Технический канал утечки представляет собой совокупность чего?
12. Какие сигналы называют опасными сигналами?
13. Перехват конфиденциальной информации - это использование несанкционированного доступа для получения конфиденциальной информации в обход и в ущерб чьим интересам?
14. Что понимается под посторонними проводниками?
15. За счет чего возникают естественные технические каналы утечки?
16. За счет чего возникают искусственные (специально создаваемые) технические каналы утечки?
17. Какое помещение называется выделенное?
18. Акустический технический канал утечки информации, в котором средой распространения акустических сигналов является воздух как называется?
19. Как производится перехват информации по прямому акустическому каналу?
20. Что можно выделить структурно в прямом акустическом канале утечки конфиденциальной информации (КИ) ?

Составил преподаватель Скряго О.С.