МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дагестанский государственный университет»

Колледж

УТВЕРЖДАЮ
Директор Колледжа ДГУ
_____ Д.Ш. Пирбудагова
«15» 08 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

профессионального модуля

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Махачкала - 2021

Составитель/ составители:

Ахмедова З.Х. - доцент кафедры ИТ и БКС факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова М.И. - преподаватель кафедры естественно-научных и гуманитарных дисциплин Колледжа ФГБОУ ВО «Дагестанский государственный университет»

Шахбанова З.И. - к.э.н., доцент кафедры прикладной информатики в экономике факультета информатики и информационных технологий ФГБОУ ВО «Дагестанский государственный университет»

Фонд оценочных средств рассмотрен и рекомендован к утверждению на заседании кафедры специальных дисциплин колледжа ДГУ

Протокол №__1__от «31» __08__2021г.

Зав. кафедрой _____/Магомедова А.М./

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

профессионального модуля

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

№	Контролируемые разделы, темы, модули	Код контролируемой компетенции	Наименование оценочного средства
МДК.02.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ			
1.	**Раздел I** Концепции инженерно-технической защиты информации	ОК 2; ОК5; ОК 6; ОК ; ОК 10.	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
2.	**Раздел II** Физические основы защиты информации	ПК 3.1; ПК 3.2; ПК 3.3; ПК3.4; ПК 3.5.	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
3.	**Раздел III** Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей	ОК 6; ОК 9; ОК 10. ПК 3.1; ПК 3.2; ПК 3.3; ПК 3.5.	Подготовка рефератов; коллоквиум; тестирование; подготовка эссе.
МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ			
1.	**Раздел 1.** Концепции инженерно-технической защиты	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК.	Комбинированный метод контроля в форме индивидуального,

	информации	3.1, ПК 3.2, ПК 3.3., ПК 3.4., ПК 3.5.	фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
2.	**Раздел 2.** Физические основы защиты информации	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 3.1, ПК 3.2, ПК 3.3., ПК 3.4., ПК 3.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных практических работ по решению ситуационных задач.
3.	**Раздел 3.** Методы защиты от несанкционированного доступа к информации и техническим ресурсам сетей	ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10, ПК. 3.1, ПК 3.2, ПК 3.3., ПК 3.4., ПК 3.5.	Комбинированный метод контроля в форме индивидуального, фронтального опроса и самостоятельной работы; тестирование; рефераты; составление и оформление письменных документов; подготовка и защита рефератов; экспертная оценка результатов выполнения индивидуальных

			практических работ по решению ситуационных задач.

Примерный перечень оценочных средств

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	**2**	**3**	**4**
1.	Деловая и/или ролевая игра	Совместная деятельность группы обучающихся и педагогического работника под управлением педагогического работника с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема), концепция, роли и ожидаемый результат по каждой игре
2.	Кейс-задача	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задачи
3.	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования педагогического работника с обучающимися.	Вопросы по темам/разделам дисциплины
4.	Контрольная работа	Средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.	Комплект контрольных заданий по вариантам
5.	Круглый стол, дискуссия,	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение	Перечень дискуссионных тем.

	полемика, диспут, дебаты	аргументировать собственную точку зрения.	
6.	Портфолио	Целевая подборка работ студента, раскрывающая его индивидуальные образовательные достижения в одной или нескольких учебных дисциплинах.	Структура портфолио
7.	Рабочая тетрадь	Дидактический комплекс, предназначенный для самостоятельной работы обучающегося и позволяющий оценивать уровень усвоения им учебного материала.	Образец рабочей тетради
8.	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умение обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированное аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.	Темы групповых и/или индивидуальных проектов
9.	Разно-уровневые задачи и задания	*Различают задачи и задания:* – репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; – реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; – творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разно-уровневых задач и заданий
10.	Расчетно-	Средство проверки умений применять	Комплект

	графическая работа	полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом.	заданий для выполнения расчетно-графической работы
11.	Реферат	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.	Темы рефератов

КРИТЕРИИ ОЦЕНКИ
по дисциплине

МДК.02.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Критерии оценки:

Оценка **«отлично»** выставляется, если студент дает полный и правильный ответ на поставленные и дополнительные (если в таковых была необходимость) вопросы:

- обнаруживает всестороннее системное и глубокое знание материала;
- обстоятельно раскрывает соответствующие теоретические положения;
- демонстрирует знание современной учебной и научной литературы;
- владеет понятийным аппаратом;
- демонстрирует способность к анализу и сопоставлению различных подходов к решению заявленной проблематики;
- подтверждает теоретические постулаты примерами из юридической практики;способен творчески применять знание теории к решению профессиональных задач;
- имеет собственную оценочную позицию и умеет аргументировано и убедительно ее раскрыть;
  четко излагает материал в логической последовательности.

Оценка **«хорошо»** выставляется, если студент дает ответ, отличающийся меньшей обстоятельностью и глубиной изложения:

- обнаруживает при этом твёрдое знание материала;
- допускает несущественные ошибки и неточности в изложении теоретического материала; исправленные после дополнительного вопроса;
- опирается при построении ответа только на обязательную литературу;
- подтверждает теоретические постулаты отдельными примерами из юридической практики;
- способен применять знание теории к решению задач профессионального характера;
- наблюдается незначительное нарушение логики изложения материала.

Оценка **«удовлетворительно»** выставляется, если студент в основном знает программный материал в объёме, необходимом для предстоящей работы по профессии, но ответ, отличается недостаточной полнотой и

обстоятельностью изложения:

- допускает существенные ошибки и неточности в изложении теоретического материала;
- в целом усвоил основную литературу;
- обнаруживает неумение применять государственно-правовые принципы, закономерности и категории для объяснения конкретных фактов и явлений;
- требуется помощь со стороны (путем наводящих вопросов, небольших разъяснений и т.п.);
- испытывает существенные трудности при определении собственной оценочной позиции;
- наблюдается нарушение логики изложения материала.

Оценка «неудовлетворительно» выставляется, если студент обнаруживает незнание или непонимание большей или наиболее существенной части содержания учебного материала:

- не способен применять знание теории к решению задач профессионального характера;
- не умеет определить собственную оценочную позицию;
- допускает грубое нарушение логики изложения материала.
- допускает принципиальные ошибки в ответе на вопросы;
- не может исправить ошибки с помощью наводящих вопросов;

Кейс-задача

по дисциплине «Техническая защита информации»

Задание

- разработать демонстрационную ЭС по подбору комплектации персонального компьютера с учетом вида профессиональной деятельности пользователя, необходимого ему программного обеспечения, хобби и приемлемого диапазона цен;

- разработать демонстрационную ЭС по выбору места отдыха с учетом количества спутников, времени года, типа отдыха, показателей здоровья, диапазона цен и т.п.

Вопросы к экзамену по дисциплине «Техническая защита информации»:

1 вопрос.

1. Предмет и задачи технической защиты информации.
   Основные параметры системы защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности.
   Системный подход при решении задач инженерно-технической защиты информации.
3. Задачи и требования к способам и средствам защиты информации техническими средствами.
4. Принципы системного анализа проблем инженерно-технической защиты информации.
   Классификация способов и средств защиты информации.
5. Особенности информации как предмета защиты.
6. Свойства информации.
7. Виды, источники и носители защищаемой информации.
8. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
9. Понятие об опасном сигнале. Источники опасных сигналов.
10. Основные и вспомогательные технические средства и системы.
11. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.
12. Понятие и особенности утечки информации.
13. Структура канала утечки информации. Характеристика каналов утечки информации.
14. Классификация существующих физических полей и технических каналов утечки информации.
15. Радиоэлектронный каналы утечки информации, характеристика.
16. Оптический канал утечки информации, характеристика.
17. Акустический каналы утечки информации, характеристика.
18. Материально-вещественный канал утечки информации, характеристика.
19. Основные виды угроз информации
20. Физические основы побочных электромагнитных излучений и наводок.
21. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств.
22. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
23. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.
24. Технические средства акустической разведки.
25. Технические средства для уничтожения информации и носителей информации, порядок применения.
26. Этапы эксплуатации технических средств защиты информации
    Установка и настройка технических средств защиты информации.

27. Классификация демаскирующих признаков
28. Телевизионные системы наблюдения. Приборы ночного видения.

2 вопрос.

1. Скрытие речевой информации в каналах связи.
2. Непосредственное подслушивание звуковой информации.
3. Система защиты от утечки по акустическому каналу (Энергетическое скрытие акустических сигналов).
4. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.
5. Прослушивание информации направленными микрофонами.
6. Электронные стетоскопы.
7. Лазерные системы подслушивания.
8. Гидроакустические преобразователи.
9. Системы защиты информации от утечки по вибрационному каналу.
10. Негласная запись информации на диктофоны.
11. Системы защиты от диктофонов.
12. Системы защиты информации от утечки по вибрационному каналу .
13. Прослушивание информации от радиотелефонов.
14. Прослушивание информации от работающей аппаратуры.
15. Прослушивание информации от радиозакладок.
16. Прослушивание информации о пассивных закладок.
17. Системы защиты от утечки по электромагнитному каналу.
18. Системы защиты от утечки от радиозакладок.
19. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
20. Использование микрофона телефонного аппарата при положенной телефонной трубке.
21. Утечка информации по сотовым цепям связи.
22. Низкочастотное устройство съема информации.
23. Высокочастотное устройство съема информации.
24. Защиты информации от несанкционированной утечки по электросетевому каналу.
25. Защиты информации от несанкционированной утечки по проводному каналу.
26. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Организация ремонта технических средств защиты информации.
27. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
28. Система защиты информации по оптическому каналу.

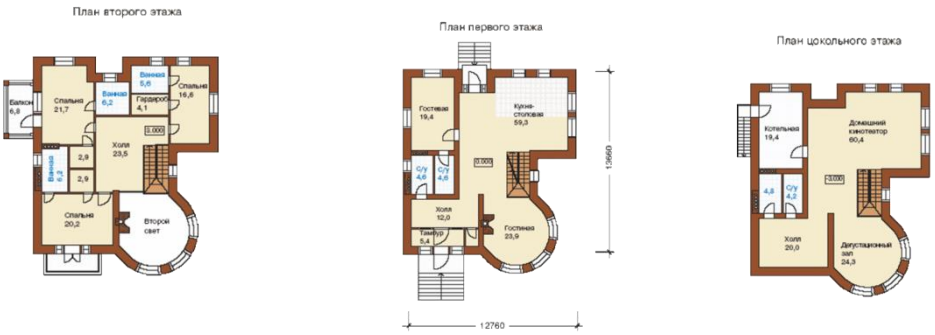
Практические вопросы:

На планах объекта.

1. Выявить и описать потенциальные каналы утечки информации в помещениях, представленных на схеме. Указать причины возникновения. Составить модель каналов утечки.
2. Для помещений, представленных на схеме, определить основные источники информации и их носители. Классифицируйте и опишите категории помещений.
3. На рисунке представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Определите группы и виды каналов утечки. Опишите технические средства, с помощью которых может быть осуществлен перехват информации.
4. Опишите возможные каналы утечки информации. Опишите методы и средства технической защиты, которые могут применяться для блокирования угроз, связанных с утечкой информации.
5. Для объекта защиты, представленного на рисунке, составьте список потенциальных угроз безопасности. Составьте план защиты объекта с помощью технических средств. Поясните расположение и обоснуйте свой выбор.
6. Для объекта защиты, представленного на рисунке, выделите и опишите контролируемы зоны ОТСС.
7. Для помещения (объекта защиты) представленного на рисунке составить проект технической защиты информации от утечки по акустическому каналу.
8. Для помещения (объекта защиты) представленного на рисунке составить проект технической защиты информации от утечки по оптическому каналу.
9. Для объекта защиты, представленного на рисунке, опишите возможные технические каналы утечки информации. Составьте модель каналов утечки и опишите среду распространения.
10. Для помещения, представленного на рисунке составьте список демаскирующих признаков. Классифицируйте выделенные признаки. Определите назначение и тип помещения.
11. Составьте проект защиты информации от утечки по акустическому каналу с использованием инженерно-технических средств защиты.
12. Составьте проект защиты информации от утечки по виброакустическому каналу с использованием инженерно-технических средств защиты.

Практические задания по дисциплине «Техническая защита информации»:

1. Подготовить к работе прибор СРМ-700 с ИК датчиком и провести обследование помещения.
2. Подготовить к работе прибор СРМ-700 с НЧ датчиком и провести обследование помещения на наличие закладного устройства.
3. Подготовить к работе прибор СРМ-700 с УВЧ датчиком и провести обследование помещения.
4. Подготовить к работе прибор ST-031 с ИК датчиком и провести обследование помещения для обнаружения ТКУИ.
5. Подготовить к работе прибор ST-031 с НЧ датчиком и провести обследование помещения.
6. Подготовить к работе прибор ST-033 с ИК датчиком и провести обследование помещения.
7. Подготовить к работе прибор ST-033 с НЧ датчиком и провести обследование помещения.
8. Подготовить к работе прибор ST-033 с ВЧ датчиком и провести обследование помещения.
9. Подготовить к работе нелинейный локатор и провести обследование помещения.
10. Подготовить к работе индикатор поля и провести обследование помещения.
11. Подготовить к работе прибор ST-152 и провести мониторинг помещения с поисковым прибором .
12. Подготовить к работе прибор ST-110 и провести мониторинг помещения с нелинейным локатором после определения района поиска.
13. Подготовить к работе прибор ST-152 и провести анализ ЭМИ за определенный период.
14. Провести анализ ЭМИ и с помощью сканирующего приемника IC-6R и провести мониторинг помещения.
15. Подготовить к работе универсальный прибор и провести поиск видеокамер и анализ наличия ЭМИ излучателей.
16. Подготовить к работе виброакустический излучатель и рассчитать потребное их количество для защиты помещения .
17. Подготовить к работе прибор АКС-1201 и провести обследование помещения на предмет наличия закладных устройств.
18. Подготовить к работе генераторы шумов и провести полное зашумление помещения для сотовой связи и интернета.
19. Подготовить к работе генераторы шумов и провести полное зашумление помещения для сотовой связи.
20. Подготовить к работе и провести поиск оптических приборов наблюдения в помещении.
21. Рассчитать требуемое кол-во ГШ-1000 для зашумления помещения с ПК если его размеры следующие длина 20 м ширина 6 м.
22. Рассчитать требуемое количество оборудования для закрытия речевого канала утечки информации в здании имеющего следующие характеристики



Технология оценивания компетенций фондами оценочных средств: формирование критериев оценивания компетенций;

Ознакомление обучающихся в ЭИОС с критериями оценивания конкретных типов оценочных средств; оценивание компетенций студентов с помощью оценочных средств программы практики - защита отчета по практике в форме собеседования; публикация результатов освоения ОПОП в личном кабинете в ЭИОС обучающегося;

Комплект тестов (тестовых заданий) по дисциплине «Техническая защита информации»:

Тест для формирования «Знать» компетенции ОК1-ОК6

Вопрос №1. К основным видам политики безопасности не относится следующая:

Варианты ответов:

а) дискреционная
б) матричная (двухмерная)
в) трехмерная
г) избирательная

Вопрос №2. В соответствии с действующим законом «конфиденциальность информации» определяется как:

Варианты ответов:

а) свойство информации, позволяющее ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
б) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
в) свойство информации, доступ к которой ограничивается в соответствии с законодательством РФ
г) обязательное для соблюдения физическим или юридическим лицом требование не допускать распространение информации без согласия её обладателя

Вопрос №3. Для информационно-телекоммуникационных сетей не характерен следующий канал доступа к информации, использующий:
Варианты ответов:

а) терминалы пользователей и администратора системы
б) стеганографические средства
в) средства загрузки программного обеспечения в вычислительный комплекс 4. средства отображения информации

Вопрос №4. Оценка рисков для ИС не производится с помощью следующей шкалы:

Варианты ответов:

а) количественной
б) логарифмической
в) матричной
г) качественной

Вопрос №5. Основным признаком классификации угроз ИБ является:
Варианты ответов:

а) источники угроз
б) направленность угроз
в) вид наносимого реализацией угрозы ущерба
г) средства, применяемые для реализации угроз

Критерии оценки выполнения задания

Неудовлетворительно от 0% до 30% правильных ответов из общего числа тестовых заданий

Удовлетворительно от 31% до 50% правильных ответов из общего числа тестовых заданий

Хорошо от 51% до 80% правильных ответов из общего числа тестовых заданий

Отлично от 81% до 100% правильных ответов из общего числа тестовых заданий

Опрос для формирования «Уметь» компетенции ОК4 1.

1. Понятие информационной безопасности и защиты информации.
2. Государственная система защиты информации в России.
3. Классификация тайн по характеру относимых к ним сведений.
4. Классификация компьютерных преступлений.
5. Базовые свойства информации, подлежащие защите.
6. Основные уровни обеспечения информационной безопасности.
7. Классификация угроз информационной безопасности.
8. Концептуальные нормативно-правовые акты в области защиты информации.
9. Понятие политики ИБ и основные этапы её разработки.
10. Базовые виды политики ИБ и их краткое описание.
11. Основные угрозы компьютерным системам.
12. Методики оценки рисков для ИС.
13. Стандарты в области разработки политики ИБ и анализа рисков.
14. Инструментальные средства для анализа рисков и управления ими.
15. Основные сервисы программных средств защиты информации в ИС.
16. Базовые группы методов аутентификации.
17. Основные рекомендации по формированию паролей.
18. Биометрические системы идентификации пользователей.
19. Основные виды управления доступом к информации.
20. Классификация компьютерных вирусов.
21. Симметричные и ассиметричные криптосистемы.
22. Основные методы шифрования данных.
23. Базовые криптографические стандарты.
24. Сервисы безопасности для реализации защитных функций в сети.

Критерии оценки выполнения задания

Неудовлетворительно Обучающийся обнаруживает незнание ответа на вопросы, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал

Удовлетворительно Обучающийся обнаруживает знание и понимание основных положений заданных вопросов, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил, не

умеет достаточно обосновать свои суждения и привести примеры, излагает материал непоследовательно и допускает ошибки

Хорошо Обучающийся дает правильные ответы на вопросы, но допускает 1-2 ошибки, которые сам же исправляет, не умеет достаточно глубоко и доказательно обосновать свои суждения

Отлично Обучающийся полно и аргументировано отвечает на вопросы, обнаруживает понимание материала, может обосновать свои суждения, привести необходимые примеры, излагает материал последовательно и правильно

Расчетное задание для формирования «Владеть» компетенции ПК3 1.

Оцените суммарную максимальную и суммарную минимальную величину ущерба от реализации совокупности следующих угроз:

1) неумышленные действия (ошибки) персонала;

2) атаки злоумышленников;

3) другие угрозы.

При этом первая угроза может возникнуть с вероятностью 20% (потери от её реализации с наибольшей вероятностью могут составить максимально от 1 млн. руб. до минимально 200 тыс. руб.), а соответствующие финансовые потери от каждой последующей угрозы составляют 40% от соответствующих максимальных и минимальных потерь от реализации предыдущей угрозы. Вероятность второй и третьей угрозы составляет соответственно 10% и 5%.

2. Рассчитайте, во сколько раз разнятся времена раскрытия пароля при использовании в пароле только символов стандартной клавиатуры компьютера (256 символов) или только всех букв русского алфавита, если длина пароля в первом случае составляет пять символов, а во втором – десять символов. При этом время ввода пароля во втором случае в два раза больше, чем в первом.

3. Постройте иерархическую пирамиду защищаемых ресурсов информационной системы, обозначив 1 - наиболее защищаемый ресурс, 4 - наименее защищаемый ресурс.

4. Рассчитайте, какой криптографический ключ наименее устойчив к взлому при его длине в 0,1 пикойоттабайт, 10 микро-зеттабайт или 100 нано-эксабайт.

5. Перечислите основные принципы реализации архитектурного уровня обеспечения информационной безопасности системы с указанием причин необходимости существования этого уровня.

6. Перечислите, какие одноимённые программные сервисы защиты должны быть установлены для информационно-телекоммуникационной сети и для информационной системы.

7. Проранжируйте нижеуказанные сервисы защиты информационной системы (от первоначального – 1 до заключительного - 5): идентификация и аутентификация, экранирование, разделение доступа, пассивный аудит, шифрование.

8. Перечислите, какие сервисы защиты должны быть установлены только для информационно-телекоммуникационной и не входить в число сервисов защиты для информационной системы.

9. В компании, анализируя количество выявленных угроз ИБ за 2015 г., выявили , что во 2-ом квартале таких угроз было на 40 % больше, чем в 1-ом; во 2-м полугодии обнаружено лишь 20% годового количества угроз. При этом в последнем квартале этих угроз было выявлено в два раза больше, чем в 3-ем квартале. Количество инсайдерских угроз ИБ в каждом квартале составляло 10% от всего числа угроз за квартал. Каково было количество инсайдерских угроз в каждом квартале, если общее число всех угроз во 2-ом квартале равнялось 70?

10. Составьте иерархическую систему из действующих в настоящее время понятий: компьютерная безопасность, информационная безопасность, информация, защита данных, пронумеровав их с верхнего уровня - 1 до нижнего - 4.

Критерии оценки выполнения задания

Неудовлетворительно Задание выполнено не полностью и объем выполненной части работы не позволяет сделать правильных выводов

Удовлетворительно Задание выполнено не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо Задание выполнено в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или

не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя

Отлично Задание выполнено в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя

Тест для формирования «Знать» компетенции ПК3.4

Вопрос №1. Наиболее высокий уровень защиты информации обеспечивает межсетевой экран следующего класса:

Варианты ответов:

а) 1
б) 2
в) 3
г) 4

Вопрос №2. К основным мерам по защите криптографических ключей не относится следующая:

Варианты ответов:

а) ограничение круга лиц, допущенных к работе с ключами
б) регламентация рассылки, хранения и уничтожения ключей
в) регламентация порядка смены ключей
г) применение математического метода конгруэнтных сечений для хранения ключей

Вопрос №3. Специалисты в области криптографии не занимаются: Варианты ответов:

а) созданием программно-технических комплексов закрытия информации
б) исследованием возможности расшифровывания информации без знания ключей
в) созданием технических средств закрытия информации
г) поиском и исследованием математических методов преобразования информации

Вопрос №4. Для шифрования коммерческой информации с использованием алгоритма RSA рекомендуется следующая длина ключа (в битах):

Варианты ответов:

а) 512
б) 768
в) 1024

г) 2048

Вопрос №5. Процесс реализации стеганографической защиты включает следующее число этапов:

а) Варианты ответов:
   a. три
   b. четыре
   c. пять
   d. шесть
   e.

Критерии оценки выполнения задания

Неудовлетворительно от 0% до 30% правильных ответов из общего числа тестовых заданий

Удовлетворительно от 31% до 50% правильных ответов из общего числа тестовых заданий

Хорошо от 51% до 80% правильных ответов из общего числа тестовых заданий

Отлично от 81% до 100% правильных ответов из общего числа тестовых заданий

Практическое задание для формирования «Уметь» компетенции ПК3.5

Составьте конспект для проведения занятия по одной из указанных тем: (при составлении конспекта используйте не менее 5 источников литературы)

1. Классификация информации. Виды данных и носителей.
2. Ценность информации. Цена информации.
3. Количество и качество информации.
4. Виды защищаемой информации.
5. Демаскирующие признаки объектов защиты.
6. Классификация источников и носителей информации.
7. мероприятия по управлению доступом к информации.
8. Функциональные источники сигналов. Опасный сигнал.
9. Основные средства и системы, содержащие потенциальные источники опасных сигналов.
10. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
11. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
12. Виды угроз безопасности информации.
13. Основные принципы добывания информации.
14. Процедура идентификации, как основа процесса обнаружения объекта. 15.

Методы синтеза информации.
15. Методы несанкционированного доступа к информации.
16. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
17. Способы наблюдения с использованием технических средств.
18. Каналы утечки информации. Технические каналы утечки
19. Классификация технических каналов утечки по физической природе носителя.
20. Классификация технических каналов утечки по информативности.
21. Классификация технических каналов утечки по времени функционирования.
22. Классификация технических каналов утечки по структуре.
23. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
24. Перехват электромагнитных излучений.
25. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
26. Понятия скрытия информации, виды скрытий. Информационный портрет.
27. Противодействие наблюдению. Способы маскировки.
28. Способы и средства противодействия подслушиванию.
29. Нейтрализация закладных устройств.
30. Состав инженерной защиты и технической охраны объектов.
31. Инженерные конструкции и сооружения для защиты информации. Их классификация.
32. Средства идентификации личности.
33. Классификация датчиков охранной сигнализации
34. Классификация извещателей.
35. Телевизионные системы наблюдения.
36. Основные средства системы видеоконтроля.
37. Защита личности как носителя информации.
38. Системный подход к защите информации.

Критерии оценки выполнения задания

Неудовлетворительно Работа выполнена не полностью и объем выполненной части работы не позволяет сделать правильных выводов

Удовлетворительно Работа выполнена не полностью, но не менее 50% объема, что позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки

Хорошо Работа выполнена в полном объеме с соблюдением необходимой последовательности действий, но допущена одна ошибка или не более двух недочетов и обучающийся может их исправить самостоятельно или с небольшой помощью преподавателя

Отлично Работа выполнена в полном объеме без ошибок с соблюдением необходимой последовательности действий

Презентация для формирования «Владеть» компетенции ПК3 1. по дисциплине «Техническая защита информации»:

1. Параметры системы защиты информации.
2. Этапы проектирования системы защиты информации.
3. Потенциальные каналы утечки информации.
4. Этапы разработки мер по предотвращению угроз утечки информации.
5. Угрозы сохранности данных в компьютере случайного характера
6. Устройства электропитания компьютера, применяемые для защиты компьютера от неблагоприятных воздействий питающей электросети.
7. Дефекты магнитных дисков.
8. Простые приемы, используемые для защиты компьютера от умышленных действий.
9. Классификация вирусов.
10. Классификация антивирусных программ.
11. Компьютерная преступность. Виды преступной деятельности.
12. Преступления, связанные с нарушением частной тайны.
13. Информационные процессы.
14. Информационные технологии и их основные свойства.
15. Понятия сигнала, сообщения и данных.
16. Методы защиты информации от преднамеренного доступа.
17. Методы обеспечения безопасности каналов передачи данных.
18. Методы обеспечения достоверности передачи информации (методов защиты от ошибок).
19. Механизмы обеспечения безопасности радиолиний.
20. Криптографическая защита информации (основные понятия).
21. Методы шифрования данных.
22. Стандарт шифрования данных DES.

Критерии оценки выполнения задания

Неудовлетворительно В презентации не раскрыто содержание представляемой темы; имеются фактические (содержательные), орфографические и стилистические ошибки. Не представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем не соответствуют требованиям реализации принципа наглядности в обучении

Удовлетворительно Презентация включает менее 8 слайдов основной части. В презентации не полностью раскрыто содержание представляемой

темы, нечетко определена структура презентации, имеются содержательные, орфографические и стилистические ошибки (более трех), представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем соответствуют требованиям реализации принципа наглядности в обучении

Хорошо Презентация включает менее 12 слайдов основной части. В презентации не полностью раскрыто содержание представляемой темы, четко определена структура презентации, имеются незначительные содержательные, орфографические и стилистические ошибки (не более трех), представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем в полной мере соответствуют требованиям реализации принципа наглядности в обучении

Отлично Презентация включает не менее 12 слайдов основной части. В презентации полностью и глубоко раскрыто содержание представляемой темы, четко определена структура презентации, отсутствуют фактические (содержательные), орфографические и стилистические ошибки, представлен перечень источников. Цветовые, шрифтовые решения, расположение текстов и схем соответствуют требованиям реализации принципа наглядности в обучении

Темы эссе (рефератов, докладов, сообщений) по дисциплине «Техническая защита информации»:

1. Понятие и сущность информационной безопасности и защиты информации 1. Необходимость и значимость нормативно-правового определения основных понятий. 2. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.
2. Основные угрозы информационной безопасности. Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия.
3. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. 8. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС).
4. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.

5. Правовой уровень обеспечения информационной безопасности.
6. Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации.
7. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну.
8. Место коммерческой тайны в системе предпринимательской деятельности.
9. Основания и методика отнесения сведений к коммерческой тайне.
10. Степени конфиденциальности сведений, составляющих коммерческую тайну.
11. Методика формирования на фирме перечня сведений, относящихся к коммерческой тайне.
12. Административный уровень обеспечения информационной безопасности
13. Концепция ИБ, её цели и этапы построения. 18. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии
14. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики ИБ.
15. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков.
16. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.
17. Программно-технический уровень обеспечения защиты информации
18. Программные сервисы защиты информации в ИС.
19. Идентификация и аутентификация пользователей как передовой рубеж защиты информации
20. Базовые методы парольной аутентификации. Модели разграничения доступа к информации.
21. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности.
22. Базовые методы криптографического преобразования данных. 28. Потоковое и блочное шифрование.
23. Процедура формирования электронной подписи
24. Экранирование информации в информационно-телекоммуникационных сетях (ИТС).
25. Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.
26. Процедурный уровень информационной безопасности. Процедурный уровень, назначение, цели и задачи процедурного уровня ИБ. Перечислите основные классы мер процедурного уровня
27. Основные правила по управлению персоналом, принцип разделение обязанностей и минимизация.
28. Физическая защита: цели и задачи по организации и управлению физической

защиты.

29. Цели и задачи по поддержанию работоспособности информационных систем, Перечислите основные положения по реагированию нарушений режима безопасности и планированию восстановительных работ.
30. Система защиты информации. Что понимается под комплексным подходом к защите информации. Что понимается под системным подходом к защите информации. Опишите типовую структура системы защиты информации на предприятиях и от чего она зависит. Перечислите порядок и этапы по созданию системы защиты информации
31. Методы (виды) обеспечения системы защиты информации. Цели и задачи системы управлении и организации работ по обеспечению безопасности информации на предприятии. Задачи и функции, возлагаемые на руководителей и должностных лиц в решении задач по организационной защите информации
32. Структура системы защиты информации на предприятии, перечислите состав подразделений, цели и основные задачи.
33. Обеспечение режима конфиденциальности при работе с защищаемой информацией. Порядок разработки ведомственного перечня сведений конфиденциального характера. Какие сведения относятся, а какие не могут быть отнесены конфиденциальной информации? Кто и как определяют наличие сведений конфиденциального характера при разработке документа?
34. Порядок снятия грифа (пометки) конфиденциальности с документа, носителя сведений конфиденциального характера. Причины и условия, которые могут привести к нарушению режима конфиденциальности, защиты информации
35. Основания для допуска работника к сведениям, конфиденциального характера.
36. Обязанности работника фирмы в части охраны конфиденциальной информации. Обязанности работодателя в части охраны конфиденциальной информации
37. Порядок допуска работников сторонних организаций (командировочных) к сведениям конфиденциального характера. Организация совещаний с представителями сторонних организаций по конфиденциальным вопросам.
38. Порядок передачи сведений конфиденциального характера в сторонние организации.
39. Контроль за соблюдением требований информационной безопасности и защиты. Назначение, цель и задачи
40. Принципы и методы контроля режима конфиденциальности и защиты информации. Основные положения по организации и порядку проведения контроля режима конфиденциальности и защиты
41. Права и обязанности работника контроля при проверке состояния режима конфиденциальности и защиты
42. Порядок проверки наличия конфиденциальных документов и иных носителей конфиденциальных сведений. Служебная проверка (расследование) по фактам нарушения требований режима конфиденциальности.

43. Назначение акта проверки, порядок составления акта, структура и содержание акта.
44. Ответственность за правонарушения информационной безопасности и защиты информации.
45. За какие виды посягательств на государственную тайну УК РФ устанавливает уголовную ответственность?
46. Что является разглашением государственной тайны?
47. Какие меры уголовной ответственности предусмотрены за компьютерные преступления?
48. За какие правонарушения в области информационной безопасности предусмотрена административная ответственность?
49. Нормативные документы, определяющие меры наказания
50. Какие виды правонарушения являются основанием для привлечения работника к ответственности
51. Виды наказания: дисциплинарные, административные, уголовные.. Меры ответственности за нарушения режима секретности и защиты государственной тайны в соответствии с УК РФ.
52. Меры ответственности за нарушения режима конфиденциальности и защиты конфиденциальной информации в соответствии с КАП и УК РФ. Меры ответственности за нарушения в сфере компьютерных преступлений в соответствии с УК

Уровни и критерии итоговой оценки результатов освоения дисциплины

Уровень1. Недостаточный Незнание значительной части программного материала, неумение даже с помощью преподавателя сформулировать правильные ответы на задаваемые вопросы, невыполнение практических заданий Неудовлетворительно/Не зачтено

Уровень 2. Базовый Знание только основного материала, допустимы неточности в ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач Удовлетворительно/зачтено

Уровень 3. Повышенный Твердые знания программного материала, допустимые несущественные неточности при ответе на вопросы, нарушение логической последовательности в изложении программного материала, затруднения при решении практических задач Хорошо/зачтено

Уровень 4. Продвинутый. Глубокое освоение программного материала, логически стройное его изложение, умение связать теорию с возможностью ее применения на практике, свободное решение задач и обоснование принятого решения Отлично/зачтено

Литература:

1. https://elibrary.ru - Научная электронная библиотека eLIBRARY.RU (ресурсы открытого доступа)
2. https://www.rsl.ru - Российская Государственная Библиотека (ресурсы открытого доступа)
3. https://link.springer.com - Международная реферативная база данных научных изданий Springerlink (ресурсы открытого доступа)
4. https://zbmath.org - Международная реферативная база данных научных изданий zbMATH (ресурсы открытого доступа)
5. Консультант+
6. http://www.garant.ru (ресурсы открытого доступа) Информационные справочные системы

КРИТЕРИИ ОЦЕНКИ
по дисциплине

МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Критерии оценки:

Оценка «отлично»: студент владеет знаниями предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, в логической последовательности и исчерпывающе отвечает на все вопросы, подчеркивал при этом самое существенное, умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделять в нем главное: устанавливать причинно-следственные связи. Четко формирует ответы, решает ситуационные задачи повышенной сложности, хорошо знаком с основной литературой, увязывает теоретические аспекты предмета с задачами практического характера.

Оценка «хорошо»: студент владеет знаниями дисциплины почти в полном объеме программы (имеются пробелы знаний только в некоторых, особенно сложных разделах). Самостоятельно и отчасти при наводящих вопросах дает полноценные ответы, не всегда выделяет наиболее существенное, не допускает вместе с тем серьезных ошибок в ответах, умеет решать легкие и средней тяжести ситуационные задачи.

Оценка «удовлетворительно»: студент владеет основным объемом знаний по дисциплине; проявляет затруднения в самостоятельных ответах, оперирует неточными формулировками. В процессе ответов допускаются ошибки по существу вопросов. Студент способен решать лишь наиболее легкие задачи, владеет только обязательным минимумом методов исследований.

Оценка «неудовлетворительно»: студент обнаруживает незнание ответа на соответствующее задание, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал, отмечаются такие недостатки в подготовке студента, которые являются серьезным препятствием к успешному овладению последующим материалом.

Вопросы к дифференцированному зачету по дисциплине «Инженерно-технические средства физической защиты объектов информатизации»:

1. Основные понятия и определения. Системный подход к защите информации
2. Основные концептуальные положения инженерно-технической защиты информации
3. Характеристики технической разведки
4. Технические каналы утечки информации
5. Методы инженерной защиты и технической охраны объектов
6. Методы скрытия информации и ее носителей
7. Физические основы побочных излучений и наводок
8. Распространение сигналов в технических каналах утечки информации
9. Средства технической разведки
10. Средства инженерной защиты и технической охраны
11. Основные задачи инженерно-технической защиты информации. Факторы, влияющие на эффективность инженерно-технической защиты информации.
12. Общая классификация акустического технического канала утечки информации.
13. Базовые принципы инженерно-технической защиты информации (общие, специальные, дополнительные).
14. 4. Воздушный акустический технический канал утечки информации. Микрофоны.
15. Показатели эффективности инженерно-технической защиты информации.
16. Воздушный акустический технический канал утечки информации. Регистрирующие устройства.
17. Основные направления инженерно-технической защиты информации.
18. Вибрационный акустический технический канал утечки информации.
19. Основные направления инженерно-технической защиты информации.
20. Электроакустический и параметрический технические каналы утечки информации.

Правила выполнения практических работ:

При выполнении практических работ (ПР), студенты должны соблюдать и выполнять следующие правила:

1. Прежде, чем приступить к выполнению ПР, обучающийся должен подготовить ответы на теоретические вопросы к ПР.
2. Перед началом каждой работы проверяется готовность обучающегося к ПР.

3. После выполнения ПР студент должен представить отчет о проделанной работе в рабочей тетради или в собственном файле (в ПК) и подготовиться к обсуждению полученных результатов и выводов.
4. Студент (обучающийся), пропустивший выполнение ПР по уважительной или неуважительной причинам, обязан выполнить работу в дополнительно назначенное время.
5. Оценка за ПР выставляется с учетом предварительной подготовки к работе, доли самостоятельности при ее выполнении, точности и грамотности оформления отчета по работе.

Критерии оценки практических работ

Практические работы оцениваются по пятибалльной шкале.

Оценка «отлично»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, необходимые программы запущены и работают без ошибок; работа оформлена аккуратно;

Оценка «хорошо»: ставится, если ПР выполнена в полном объеме, в соответствии с заданием, с соблюдением последовательности выполнения, частично с помощью преподавателя, присутствуют незначительные ошибки при запуске и эксплуатации (работе) необходимых программ; работа оформлена аккуратно;

Оценка «удовлетворительно»: частично с помощью преподавателя, присутствуют ошибки при запуске и работе требуемых программ; по оформлению работы имеются замечания.

Оценка «неудовлетворительно»: ставится, если обучающийся не подготовился к ПР, при запуске и эксплуатации (работе) требуемых программ студент допустил грубые ошибки, по оформлению работы имеются множественные замечания.

Практические задания по дисциплине «Инженерно-технические средства физической защиты объектов информатизации»:

Практическая работа №1.

Задание:

Торгово-посреднической фирмы «Столица». Бизнес этого предприятия предельно прост: «покупай дешевле – продавай дороже», или состыкуй продавца и покупателя и получи «комиссионные». Основной упор фирма

делает на закупки продуктов питания в других регионах страны и за рубежом – там, где они производятся и стоят дешевле, чем в нашем регионе. Часть продукции может быть закуплена и у местных продавцов. В этом случае фирма получает прибыль за счет того, что крупные партии товара стоят дешевле, чем мелкие. Так как в данной сфере количество фирм на сегодняшний день увеличивается, то маркетинговой политики предприятия охраняется как службой безопасности, так и лично руководством.

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 Данных о защищаемой информации.

Используя Corel DRAW произведите моделирование объектов защиты.

Эл. инф**.**
Элементы информации
Гриф КИ
Цена инф, руб.
Носитель информации
Местоположение источника информации

Практическая работа №2.

Задание:

Отдел вневедомственной охраны квартир обеспечивает электронную охрану квартир граждан в одном районе города. Для установки охранной сигнализации требуется наличие квартирного телефона. Условия установки системы охраны, ее свойства и методы оговариваются в договоре, условия договора строго конфиденциальны и индивидуальны для каждого партнера

Определите объекты и субъекты системы безопасности предприятия.

Выберите и обоснуйте виды охраны предприятия.

Составьте схему классификации в виде графа-структуры, нулевой (верхний) уровень иерархии который соответствует понятию "защищаемая информация", а n-ый (нижний) - элементам информации одного источника из перечня источников организации. Основные требования к схеме классификации: общий признак и полнота классификации, отсутствие пересечений между элементами классификации одного уровня (одна и та же информация не должна указываться в разных элементах классификации).

На основе схемы сформирует таблицу №1 **Данных о защищаемой информации.**

Используя Corel DRAW произведите моделирование объектов защиты.

Эл. инф**.**

Элементы информации

Гриф КИ

Цена инф, руб.

Носитель информации

Местоположение источника информации

1) Внимательно прочитайте задание
2) Определите объекты и субъекты охраны
3) Составьте проектную документацию по необходимому оборудованию, для организации модели защиты.
4) Создайте модель защиты объекта в Corel DRAW

Критерии оценки эссе (рефератов, докладов, сообщений)

Оценка «отлично»: выполнены все требования к написанию и защите реферата: обозначена проблема и обоснована ее актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объем, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы.

Оценка «хорошо»: основные требования к реферату и его защите выполнены, но при этом допущены недочеты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объем реферата; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы.

Оценка «удовлетворительно»: имеются существенные отступления от требований к реферированию. В частности: тема освещена лишь частично; допущены фактические ошибки в содержании реферата или при ответе на дополнительные вопросы.

Оценка «неудовлетворительно»: тема освоена лишь частично; допущены грубые ошибки в содержании реферата или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. Тема реферата не раскрыта, обнаруживается существенное непонимание проблемы.

Темы для эссе (рефератов, докладов, сообщений) по дисциплине «Инженерно-технические средства физической защиты объектов информатизации»:

1) «Направление комплексного проектирования систем защиты информации»
2) «Основные проблемы реализации систем защиты информации»
3) «Требования к КСЗИ»
4) «Задачи стратегии защиты информации»
5) «Верификация»
6) «Дискреционный контроль доступа»
7) «Биометрическая идентификация»
8) «Биометрия по клавиатурному почерку»
9) «Классификация признаков голоса и речи»
10) «Средства высоконадежной биометрической аутентификации»
11) «Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников»
12) «Меры по защите информации внутри зоны»
13) «Автоматическое обнаружение движущегося нарушителя»
14) «Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведки»
15) «Контроль эффективности инженерно-технической защиты информации»
16) «Пути оптимизации мер инженерно-технической защиты информации»
17) Принципы оценки эффективности инженерно-технической защиты информации»
18) «Источники опасных сигналов»
19) «Типы побочных излучений и наводок, возможные «антенны»»
20) «Помехи»
21) «Физические основы побочных излучений и наводок»
22) «Возможные наводки в аппаратуре»
23) «Особенности распространения сигналов в помещениях»
24) Ознакомление и литературой описывающей сканирующие приемники. Изучение инструкции сканера.
25) Ознакомление с литературой описывающей нелинейные локаторы. Изучение инструкции нелинейного локаторы.
26) Ознакомление с литературой и Интернет-ресурсами по теме космической и авиаразведки.

СТРУКТУРА ИТОГОВОГО ТЕСТА:

Тест содержит 20 вопросов случайным образом выбранных их списка. Тест проводиться на персональном компьютере в оболочке для тестирования

MyTest. Результат выдается сразу после тестирования и формируется отчет протестированных студентов на сервере.

Время на подготовку и выполнение:

Выполнение – 20 минут. За правильный ответ выставляется по 1 баллу, затем результаты суммируются, и выставляется оценка. За неправильный ответ 0 баллов.

Критерии оценки промежуточной аттестации:

Оценка «отлично» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «отлично», средний балл по аттестациям не ниже 4,5.

Оценка «хорошо» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «хорошо», средний балл по аттестациям не ниже 3,5.

Оценка «удовлетворительно» выставляется, если имеются все конспекты лекции, обучающимися выполнены 100% практических работ, оценка за итоговое тестирование – «удовлетворительно», средний балл по аттестациям не ниже 2,5.

Оценка «неудовлетворительно» выставляется, если имеются все конспекты лекции обучающимися выполнено менее 100% практических работ, оценка за итоговое тестирование – «неудовлетворительно», средний балл по аттестациям ниже 2,5.

Цель итогового тестирования:

Тестирование по учебной дисциплине **«Инженерно-технические средства физической защиты объектов информатизации»** предназначено для проверки теоретических знаний и понятийного аппарата, которые лежат в основе профессионального образования и найдут самое широкое применение в будущей профессиональной деятельности учащихся по специальности 10.02.05.Обеспечение информационной безопасности автоматизированных систем.

Критерии оценки знаний:

Процент правильных ответов, %	**Оценка знаний**
90-100	5 «отлично»
75-89	4 «хорошо»
60-74	3 «удовлетворительно»

Менее 60	2 «неудовлетворительно»

Список теоретических заданий для подготовки к итоговому тестированию (ТЗ) по дисциплине «Инженерно-технические средства физической защиты объектов информатизации»:

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:
   а) правовым методам защиты информации
   б) организационно-техническим методам защиты информации
   в) организационно-распорядительным методам защиты информации
   г) экономическим методам защиты информации
2. Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:
   а) собственник информации
   б) владелец информации
   в) пользователь
3. Форма допуска, требуемая для работы со сведениями особой важности является:
   а) первой формой допуска
   б) второй формой допуска
   в) третьей формой допуска
4. Форма допуска, требуемая для работы с совершенно секретными сведениями является:
   а) первой формой допуска
   б) второй формой допуска
   в) третьей формой допуска
5. Форма допуска, требуемая для работы с секретными сведениями является:
   а) первой формой допуска
   б) второй формой допуска
   в) третьей формой допуска
6. В сфере государственной тайны действует функционально-зональный принцип. Это значит, что:
   а) каждый пользователь допускается должностными лицами только к такой информации, которая требуется ему для исполнения должностных обязанностей
   б) каждый пользователь допускается должностными лицами только к информации, касающейся зоны его проживания
   в) каждый пользователь допускается должностными лицами ко всей информации, к которой у него есть форма допуска

7. Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:
    а) незаконного оборота информации
    б) взлома информации
    в) несанкционированного использования информации
8. Форма преднамеренного распространения или мнимого разглашения (утечки) неких планов и намерений, которые не отвечают реальным действиям называется:
    а) дезинформация
    б) легендирование
    в) шпионаж
9. Какое направление защиты в основном применяется для охраны материальных ценностей?
    а) инженерно-техническая
    б) организационно-техническая
    в) организационно-распорядительная
    г) нормативно-правовая
    д) экономическая
10. Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?
    а) инфракрасный светодиод лазерного принтера, посылающий кратковременные
    б) вспышки на электризованную поверхность фоточувствительного барабана
    в) модулированный по силе тока поток электронов, засвечивающий в определенном
    г) порядке пикселы люминофора электронно-лучевой трубки
    д) экран компьютерного монитора и глаза пользователя
    е) оптический канал связи
    ж) все варианты могут быть отнесены к техническим каналам связи
    з) контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
11. Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?
    а) визуально-оптический канал
    б) электромагнитный канал
    в) виброакустический канал
    г) материально-вещественный канал
12. Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:
    а) визуально-оптического канала
    б) электромагнитного канала

в) виброакустического канала
г) материально-вещественного канала

13. Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?
    а) визуально-оптический канал
    б) электромагнитный канал
    в) виброакустический канал
    г) материально-вещественный канал
14. Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:
    а) визуально-оптического канала
    б) электромагнитного канала
    в) виброакустического канала
    г) материально-вещественного канала
15. Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах
    а) визуально-оптический канал
    б) электромагнитный канал
    в) виброакустический канал
    г) материально-вещественный канал
16. Примером какого канала утечки информации служит звук голоса человека?
    а) визуально-оптического канала
    б) электромагнитного канала
    в) виброакустического канала
    г) материально-вещественного канала
17. По какому признаку делят на классы средства технической разведки (СТР) ?
    а) по дальности канала
    б) по форме допуска
    в) по мощности
    г) по степени финансирования
18. Портативные устройства для запечатления информации, скрытно проносимые на территорию объекта нарушителем на своем теле относят к …
    а) первому классу СРТ
    б) второму классу СРТ
    в) третьему классу СРТ
19. Для наблюдения за объектами информатизации из-за пределов их охраняемой или контролируемой территории используются СРТ…
    а) первого класса

б) второго класса
в) третьего класса

20. 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

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

22. 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

Основная литература:

1. Рагозин Ю.Н. Инженерно-техническая защита информации на объектах информатизации / Ю.Н. Рагозин. - Санкт-Петербург : Интермедия, 2019. - 216 с. - ISBN 978-5-4383-0182-0. - URL: https://ibooks.ru/bookshelf/374951/reading. - Текст: электронный.
2. Скрипник, Д. А. Общие вопросы технической защиты информации : учебник / Д. А. Скрипник.-3-е изд.-Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.-424 с.-ISBN 978-5-4497-0336-1.-Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт].-URL: https://www.iprbookshop.ru/89451.html.-Режим доступа: для авторизир. Пользователей.

Дополнительная литература:

1. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов.-Москва : Издательство Юрайт, 2021.-309 с.-(Высшее образование).-ISBN 978-5-534-04732-5.-Текст : электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/469866.
2. *Внуков, А. А.* Защита информации : учебное пособие для вузов / А. А. Внуков.-3-е изд., перераб. и доп.-Москва : Издательство Юрайт, 2021.-161 с.-(Высшее образование).-ISBN 978-5-534-07248-8.-Текст : электронный // Образовательная платформа Юрайт [сайт].-URL: https://urait.ru/bcode/470131
3. Петраков А.В. Основы практической защиты информации [Текст] : учеб. пособие для студентов вузов / А.В Петраков. – 2-е изд. – М. :Радио и связь, 2000. – 361с.

Интернет-ресурсы:

1. Информационно-справочная система по документам в области технической защитыинформации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11. Федеральный портал «Российское образование www.edu.ru