Министерство образования, науки и молодежной политики
Краснодарского края
Государственное бюджетное профессиональное образовательное учреждение
Краснодарского края «Пашковский сельскохозяйственный колледж»

УТВЕРЖДАЮ
Зам директора по УМР
_____Е.П. Ольховская
«28» 09 2022 г

Комплект контрольно-оценочных средств
для проведения текущей промежуточной аттестации студентов в рамках
основной профессиональной образовательной программы
по профессиональному модулю
ПМ.03 Защита информации техническими средствами

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

г. Краснодар, 2022

Комплект контрольно-оценочных средств для проведения аттестации студентов по профессиональному модулю ПМ.03 Защита информации техническими средствами разработан на основании рабочей программы образовательной учебной дисциплины, которая входит в структуру основной образовательной программы и предназначена для ее реализации в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (приказ Минобрнауки России от 09.12.2016.г. №1553, зарегистрировано в Минюсте России 26.12.2016 г., № 44938 (ред. 17.12.2020 г.))

Организация разработчик: ГБПОУ КК ПСХК

Разработчик:

Пушкарева Н.Я.	Преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшая квалификационная категория, математик, преподаватель информатики и ИКТ

Рассмотрен на заседании методического объединения
Информационных технологий
Протокол № 1 от «28» сентября 2022 г.
_____/Пушкарева Н.Я/

СОДЕРЖАНИЕ

1. Паспорт комплекта контрольно-оценочных средств.

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Защиты информации техническими средствами и соответствующие ему профессиональные компетенции, а также общие компетенции, формирующиеся в процессе освоения основной образовательной программы в целом.

Формой аттестации по профессиональному модулю является квалификационный экзамен. Экзамен (квалификационный) проводится в форме выполнения практико-ориентированных заданий.

2. Результаты освоения профессионального модуля, подлежащие проверке

2.1. Формы контроля и оценивания элементов профессионального модуля

Элемент модуля	Форма контроля и оценивания		
	Промежуточная аттестация	Рубежный контроль	Текущий контроль
МДК.03.01 Техническая защита информации	Экзамен	-	Устные ответы. Тестирование. Самостоятельные работы. Формализованное наблюдение и оценка выполнения и защиты практической работы.
МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	Дифференцированный зачет	Курсовая работа (проект)	Устные ответы. Тестирование. Самостоятельные работы. Формализованное наблюдение и оценка выполнения и защиты практической работы. Защита курсовой работы (курсового проекта).
МДК 03.03 Корпоративная защита от внутренних угроз информационной безопасности	Экзамен	-	Устные ответы. Тестирование. Самостоятельные работы. Формализованное наблюдение и оценка выполнения

			и защиты практической работы.
УП.04	Дифференцированный зачет	-	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП.04	Дифференцированный зачет	-	Оценка выполнения работ и оформления отчетной документации на производственной практике
Профессиональный модуль ПМ.04	Квалификационный экзамен		

2.2. Результаты аттестации по профессиональному модулю

В результате аттестации по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:

Профессиональные и общие компетенции Показатели оценки результата	Показатели оценки результата
ВД 3 Защита информации техническими средствами	
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	– устанавливает, производит монтаж и настройку технических средств защиты информации; – производит техническое обслуживание технических средств защиты информации; – применяет основные типы технических средств защиты информации; – применяет технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – знает порядок технического обслуживания технических средств защиты информации; – знает номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	– применяет основные типы технических средств защиты информации; – выявляет технические каналы утечки информации;

	– участвует в мониторинге эффективности технических средств защиты информации; – производит диагностику, устраняет отказы и неисправности, восстанавливает работоспособности технических средств защиты информации; – применяет технические средства для криптографической защиты информации конфиденциального характера; – применят технические средства для уничтожения информации и носителей информации; – применяет нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – знает физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – знает порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – знает методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – знает номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	– проводит измерения параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – применяет технические средства для защиты информации в условиях применения

	мобильных устройств обработки и передачи данных; – знает номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – знает структуру и условия формирования технических каналов утечки информации.
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	– проводит измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – выявляет технические каналы утечки информации; – применяет технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; – знает номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	– производит установку, монтаж и настройку, техническое обслуживание, диагностику, устранять отказы и неисправности, восстанавливает работоспособности инженерно-технических средств физической защиты; – применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применяет инженерно-технические средства физической защиты объектов информатизации; – знает основные принципы действия и характеристики технических средств физической защиты; – знает основные способы физической защиты объектов информатизации; – знает номенклатуру применяемых средств физической защиты объектов информатизации.

ПК 3.6. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах	– ставит цели, формулирует задачи, связанные с обеспечением корпоративной защиты от внутренних угроз информационной безопасности; – знает объекты компьютерных технологий, используемые в обеспечении корпоративной защиты от внутренних угроз информационной безопасности; – знает и применяет технологию анализа и защиты сетевого трафика; – осуществляет развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре.
ПК 3.7. Выявлять и анализировать возможные угрозы информационной безопасности объектов	– анализирует тенденции развития систем обеспечения корпоративной защиты от внутренних угроз информационной безопасности; – применяет знания о корпоративной защите от внутренних угроз информационной безопасности в решении поставленных задач; – применяет классификацию объектов защиты.
ПК 3.8. Ориентироваться в условиях частой смены технологий в профессиональной деятельности	– применяет понятийный аппарат информационных технологий и особенности терминологии в области корпоративной защиты от внутренних угроз информационной безопасности;
ПК 3.9. Проводить регламентные работы и фиксировать отказы средств защиты	– применяет базовые составляющие в области развития систем информационной безопасности; – проводит регламентные работы и фиксацию отказов средств защиты.
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	–распознает задачу и/или проблему в профессиональном и/или социальном контексте; –анализирует задачу и/или проблему и выделять её составные части; –определяет этапы решения задачи; –выявляет и эффективно ищет информацию, необходимую для решения задачи и/или проблемы; –составляет план действия;

	–определяет необходимые ресурсы; –владеет актуальными методами работы в профессиональной и смежных сферах; –реализует составленный план; –оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); –знает актуальный профессиональный и социальный контекст, в котором приходится работать и жить; –использует основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. –применяет алгоритмы выполнения работ в профессиональной и смежных областях; –применяет методы работы в профессиональной и смежных сферах; –использует структуру плана для решения задач; –применяет порядок оценки результатов решения задач профессиональной деятельности.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	–определяет задачи поиска информации; –определяет необходимые источники информации; –планирует процесс поиска; –структурирует получаемую информацию; –выделяет наиболее значимое в перечне информации; –оценивает практическую значимость результатов поиска; –оформляет результаты поиска; –знает номенклатура информационных источников, применяемых в профессиональной деятельности; –использует приемы структурирования информации; –применяет формат оформления результатов поиска информации.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	–определяет актуальность нормативно-правовой документации в профессиональной деятельности;

	–выстраивает траектории профессионального и личностного развития; –знает содержание актуальной нормативно-правовой документации; –применяет современную научную и профессиональную терминологию; –определяет возможные траектории профессионального развития и самообразования.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	–умеет организовать работу коллектива и команды; –умеет взаимодействовать с коллегами, руководством, клиентами; –знает психологию коллектива; –знает психологию личности; –знает основы проектной деятельности.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	–излагает свои мысли на государственном языке; –оформляет документы; –использует особенности социального и культурного контекста; –применяет правила оформления документов.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	–описывать значимость своей профессии; –презентует структуру профессиональной деятельности по специальности; –демонстрирует знание сущности гражданско-патриотической позиции; –демонстрирует знание общечеловеческих ценностей; –применяет правила поведения в ходе выполнения профессиональной деятельности.
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	–соблюдает нормы экологической безопасности; –определяет направления ресурсосбережения в рамках профессиональной деятельности по специальности; –демонстрирует знание правил экологической безопасности при ведении профессиональной деятельности; –знает основные ресурсы, задействованные в профессиональной деятельности; –знает пути обеспечения ресурсосбережения.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	–использует физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; –применяет рациональные приемы двигательных функций в профессиональной деятельности; –пользуется средствами профилактики перенапряжения характерными для данной специальности; –демонстрирует знание роли физической культуры в общекультурном, профессиональном и социальном развитии человека; –знает основы здорового образа жизни; –знает условия профессиональной деятельности и зоны риска физического здоровья для специальности; –применяет средства профилактики перенапряжения.
ОК 09. Использовать информационные технологии в профессиональной деятельности	–применяет средства информационных технологий для решения профессиональных задач; –использует современное программное обеспечение; –знает современные средства и устройства информатизации; –знает порядок их применения и программное обеспечение в профессиональной деятельности.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	–понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; –участвует в диалогах на знакомые общие и профессиональные темы; –строит простые высказывания о себе и о своей профессиональной деятельности; –кратко обосновывает и объясняет свои действия (текущие и планируемые); –пишет простые связные сообщения на знакомые или интересующие профессиональные темы;

	–применяет правила построения простых и сложных предложений на профессиональные темы; –использует основные общеупотребительные глаголы (бытовая и профессиональная лексика); –владеет лексическим минимумом, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; –знает правила чтения текстов профессиональной направленности.

3. Оценка освоения профессионального модуля:

3.1. Типовые задания для текущего контроля по МДК.03.01. Техническая защита информации

Раздел 1. Концепция инженерно-технической защиты информации

Тема 1.1. Предмет и задачи технической защиты информации

1. Перечень вопросов для устного или письменного опроса по теме:

1. Предмет и задачи технической защиты информации.
2. Характеристика инженерно-технической защиты информации как области информационной безопасности.
3. Системный подход при решении задач инженерно-технической защиты информации.
4. Основные параметры системы защиты информации.

Тема 1.2. Общие положения защиты информации техническими средствами

1. Перечень вопросов для устного или письменного опроса по теме:

1. Задачи и требования к способам и средствам защиты информации техническими средствами.
2. Принципы системного анализа проблем инженерно-технической защиты информации.
3. Классификация способов и средств защиты информации.

Раздел 2. Теоретические основы инженерно-технической защиты информации

Тема 2.1. Информация как предмет защиты

1. Самостоятельная работа

1. Особенности информации как предмета защиты.
2. Свойства информации.
3. Виды, источники и носители защищаемой информации.

2. Тестовые задания по теме:

1. *Информация это* - а. сведения, поступающие от СМИ б. только документированные сведения о лицах, предметах, фактах, событиях	2. *Информация* а. не исчезает при потреблении б. становится доступной, если она содержится на материальном носителе

в. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления г. только сведения, содержащиеся в электронных базах данных	в. подвергается только "моральному износу"
3. *Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется* а. достоверной б. конфиденциальной в. документированной г. коммерческой тайной	4. *Документы, содержащие государственную тайну снабжаются грифом* а. «секретно» б. «совершенно секретно» в. «особой важности»
5. *По принадлежности информационные ресурсы подразделяются на* а. государственные, коммерческие и личные б. государственные, не государственные и информацию о гражданах в. информацию юридических и физических лиц г. официальные, гражданские и коммерческие	6. *К негосударственным относятся информационные ресурсы* а. созданные, приобретенные за счет негосударственных учреждений и организаций б. созданные, приобретенные за счет негосударственных предприятий и физических лиц в. полученные в результате дарения юридическими или физическими лицами
7. *По доступности информация классифицируется на* а. открытую информацию и государственную тайну б. конфиденциальную информацию и информацию свободного доступа в. информацию с ограниченным доступом и общедоступную информацию г. виды информации, указанные в остальных пунктах	8. *К конфиденциальной информации относятся документы, содержащие* а. государственную тайну б. законодательные акты в. «ноу-хау» г. сведения о золотом запасе страны
9. *Запрещено относить к информации ограниченного доступа* а. информацию о чрезвычайных ситуациях б. информацию о деятельности органов государственной власти в. документы открытых архивов и библиотек	10. *К конфиденциальной информации не относится* а. коммерческая тайна б. персональные данные о гражданах в. государственная тайна г. «ноу-хау»
11. *Вопросы информационного обмена регулируются (...) правом* а. гражданским б. информационным в. конституционным г. уголовным	12. *Система защиты государственных секретов определяется Законом* а. «Об информации, информатизации и защите информации» б. «Об органах ФСБ» в. «О государственной тайне» г. «О безопасности»
13. *Конфиденциальная информация это* а. сведения, составляющие государственную тайну	14. *Какая информация подлежит защите?* а. информация, циркулирующая в системах и сетях связи

б. сведения о состоянии здоровья высших должностных лиц в. документированная информация, доступ к которой ограничивается в г. соответствии с законодательством РФ д. данные о состоянии преступности в стране	б. зафиксированная на материальном носителе информация с реквизитами, в. позволяющими ее идентифицировать г. только информация, составляющая государственные информационные ресурсы д. любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу
15. *Государственные информационные ресурсы не могут принадлежать* а. физическим лицам б. коммерческим предприятиям в. негосударственным учреждениям	16. *Классификация и виды информационных ресурсов определены* а. Законом «Об информации, информатизации и защите информации» б. Гражданским кодексом в. Конституцией
17. *Запрещено относить к информации с ограниченным доступом* а. законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны) б. только информацию о чрезвычайных ситуациях в. только информацию о деятельности органов государственной власти (кроме государственной тайны) г. документы всех библиотек и архивов	18. *Действие Закона «О государственной тайне» распространяется* а. на всех граждан и должностных лиц РФ б. только на должностных лиц в. на граждан, которые взяли на себя обязательство выполнять требования г. законодательства о государственной тайне д. на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения
19. *К коммерческой тайне могут быть отнесены* а. сведения, не являющиеся государственными секретами б. сведения, связанные с производством и технологической информацией в. сведения, связанные с управлением и финансами	20. *К государственной тайне относится...* а. информация в военной области б. информация о внешнеполитической и внешнеэкономической деятельности государства в. информация в области экономики, науки и техники и сведения в области разведывательной и оперативно-розыскной деятельности

Ключ к тесту:

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
в	а, б, в	в	а, б, в	а	а, б, в	в	а	а, б, в	г

11.	12.	13.	14.	15.	16.	17.	18.	19.	20.
а	в	в	д	а, б, в	а	а	д	а, б, в	а, б, в

3. Перечень вопросов для устного или письменного опроса по теме:

1. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
2. Понятие об опасном сигнале.
3. Источники опасных сигналов.
4. Основные и вспомогательные технические средства, и системы.

5. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.

4. Тематика практических работ:

Практическая работа № 1.

Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.

Цель работы: освоение приемов и методов анализа основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.

Тема 2.2. Технические каналы утечки информации

1. Перечень вопросов для устного или письменного опроса по теме:

1. Понятие и особенности утечки информации.
2. Структура канала утечки информации.
3. Классификация существующих физических полей и технических каналов утечки информации.
4. Характеристика каналов утечки информации.
5. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.

2. Тестовые задания – опрос по теме:

1. Что понимают под техническим каналом утечки информации?
2. Перечислите технические каналы утечки информации, обрабатываемой ТСПИ.
3. Перечислите технические каналы утечки информации при передаче ее по каналам связи.
4. Перечислите технические каналы утечки речевой информации.
5. Перечислите технические каналы утечки видовой информации.
6. Что такое контролируемая зона?
7. Что называется опасной зоной?
8. Что называется опасной зоной 1?
9. Что называется опасной зоной 2?

Ответы:

1. Что понимают под техническим каналом утечки информации?
   (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР) и физической среды, в которой распространяется информационный сигнал. В сущности, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте.
2. Перечислите технические каналы утечки информации, обрабатываемой ТСПИ:
   Электромагнитные
   Электрические
   Параметрические
   Вибрационные
3. Перечислите технические каналы утечки информации при передаче ее по каналам связи:
   Электромагнитные
   Электрические
   Индукционные

Паразитные связи

4. Перечислите технические каналы утечки речевой информации:
   Акустические
   Виброакустические
   Параметрические
   Акустоэлектрические
   Оптико-электронные
5. Перечислите технические каналы утечки видовой информации:
   Наблюдение за объектами
   Съемка объектов
   Съемка документов
6. Что такое контролируемая зона?

   Контролируемая зона -территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска. В КЗ, посредством проведения технических и режимных мероприятий, должны быть созданы условия, предотвращающие возможность утечки из нее конфиденциальной информации. КЗ определяется руководством организации, исходя из конкретной обстановки в месте расположения объекта и возможностей использования технических средств перехвата.
7. Что называется опасной зоной?
   Зона с возможностью перехвата разведывательным оборудованием побочных электромагнитных излучений, содержащих конфиденциальную информацию, называется опасной зоной.
8. Что называется опасной зоной 1?

   Пространство вокруг ТСПИ, в котором на случайных антеннах наводится информационный сигнал выше допустимого уровня, называется опасной зоной 1
9. Что называется опасной зоной 2?
   Зона, в которой возможен перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации (т.е. зона, в пределах которой отношение "информационный сигнал/помеха" превышает допустимое нормированное значение), называется (опасной) зоной 2

3. Тематика практических работ:

Практическая работа № 2.

Определение канала утечки информации. Проведение сравнительного анализа каналов.

Цель работы: освоение приемов определения каналов утечки информации, проведения сравнительного анализа каналов.

Тема 2.3. Методы и средства технической разведки

1. Перечень вопросов для устного или письменного опроса по теме:

1. Техническая разведка: определение, классификация, возможности.
2. Формы разведывательной деятельности.
3. Основные этапы и процедуры добывания информации технической разведки.
4. Классификация технических средств разведки.
5. Методы и средства технической разведки.
6. Средства несанкционированного доступа к информации.

2. Самостоятельная работа

1. Средства и возможности оптической разведки.
2. Средства дистанционного съема информации.

3. Тестовые задания – опрос по теме:

1. По направлениям разведывательной деятельности иностранные разведки подразделяется на:
2. Основные формы разведывательной деятельности:
3. Формы легальной разведки:
4. По используемыми носителями средств добывания информации, в соответствии с которым ТР делится на:
5. В зависимости от применяемых фотоматериалов фотографирование в разведывательных целях может быть:
6. Приборы ИКР делятся на группы:
7. Радиоэлектронная разведка подразделяется на виды:
8. Акустические каналы утечки информации можно разделить на:
9. Средства, устанавливаемые заходовыми (требующими проникновения на объект) методами:
10. Средства, устанавливаемые беззаходовыми методами:

Ответы:

1. По направлениям разведывательной деятельности иностранные разведки подразделяется на:

– *политическую*
– *экономическую*
– *военную и научно-техническую*

2. Основные формы разведывательной деятельности:

– *агентурная разведка*
– *легальная разведка*
– *техническая разведка*
– *аналитическая обработка первичной информации*

3. Формы легальной разведки:

– *анализ всех открытых публикаций, которые издаются в стране объекте разведки;*
– *получение информации во время непосредственных контактов агентов с интересующими их лицами на приемах, встречах, конференциях;*
– *визуальное* наблюдение, кино– и фотосъемка при перемещении иностранцев по стране

4. По используемыми носителями средств добывания информации, в соответствии с которым ТР делится на:

– *космическую*
– *воздушную*
– *морскую*
– *наземную*

5. В зависимости от применяемых фотоматериалов фотографирование в разведывательных целях может быть:

– *черно-белым*
– *цветным*

– *спектрозональным*

6. Приборы ИКР делятся на группы:

– *тепловизионные приборы*

– *приборы ночного видения (ПНВ)*

7. Радиоэлектронная разведка подразделяется на виды:

– радиоразведка

– радиотехническая разведка

– радиолокационная разведка

– телевизионная разведка

8. Акустические каналы утечки информации можно разделить на:

– воздушные

– вибрационные

– акустоэлектрические

– оптико-электронные

– параметрические

9. Средства, устанавливаемые заходовыми (требующими проникновения на объект) методами:

– радиозакладки

– закладки с передачей акустической информации в инфракрасном диапазоне

– закладки с передачей информации по сети 220 В

– закладки с передачей акустической информации по телефонной линии;

– диктофоны

– проводные микрофоны

– «телефонное ухо»

10. Средства, устанавливаемые беззаходовыми методами:

– аппаратура, использующая микрофонный эффект

– высокочастотное навязывание

– стетоскопы

– лазерные микрофоны

4. Тематика практических работ:

Практическая работа № 3.

Планирование мероприятий по определению возможных средств организации технической разведки.

Цель работы: освоение приемов планирования мероприятий по определению возможных средств организации технической разведки.

Раздел 3. Физические основы технической защиты информации

Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

1. Перечень вопросов для устного или письменного опроса по теме:

1. Физические основы побочных электромагнитных излучений и наводок.
2. Акустоэлектрические преобразования.
3. Паразитная генерация радиоэлектронных средств.
4. Виды паразитных связей и наводок.
5. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.

6. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей

2. Тестовые задания по теме:

Вариант 1

1. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?
   а) Информационная защита информации
   б) Информационная безопасность
   в) Зашита информации
2. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?
   а) Препятствие
   б) Управление доступом
   в) Маскировка
3. Какой метод защиты информации связан с регулированием использования всех ресурсов информационной системы?
   а) Маскировка
   б) Препятствие
   в) Управление доступом
4. Как называется установления подлинности объекта по предъявленному им идентификатору (имени)?
   а) Аутентификация
   б) Идентификация
   в) Маскировка
5. Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?
   а) Аутентификация
   б) Идентификация
   в) Маскировка
6. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?
   а) Принуждение
   б) Маскировка
   в) Идентификация
7. Какой метод защиты информации мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм?
   а) Принуждение
   б) Побуждение
   в) Маскировка
8. Какие средства защиты информации предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации?
   а) Аппаратные
   б) Программные

в) Физические

9. Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?

а) Аппаратные
б) Программные
в) Физические

10. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

а) Аппаратные
б) Программные
в) Физические

Вариант 2

1. Какие средства защиты информации регламентируют правила использования, обработки и передачи информации и устанавливают меры ответственности?

а) Законодательные средства
б) Организационные средства
в) Аппаратно-программные

2. Какие средства защиты информации встроены в блоки информационной системы (сервера, компьютеры и т.д.) и предназначены для внутренней защиты элементов вычислительной техники и средств связи?

а) Аппаратные
б) Программные
в) Физические

3. Какие средства защиты информации предназначены для выполнения функций защиты информационной системы с помощью программных средств?

а) Аппаратные
б) Программные
в) Физические

4. Как называются правила и нормы поведения сотрудников в коллективе, регулирующие вопросы защиты информации?

а) Организационные средства
б) Аппаратно-программные
в) Морально-этические средства

5. Как называется защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации?

а) Информационная защита информации
б) Информационная безопасность
в) Зашита информации

6. Как называется метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т.д.)?

а) Препятствие
б) Управление доступом
в) Маскировка

7. Как называется метод защиты информации в информационной системе организации путем ее криптографического закрытия?

а) Аутентификация
б) Идентификация
в) Маскировка

8. При использовании какого метода защиты пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности?

а) Принуждение
б) Маскировка
в) Идентификация

9. Какие средства защиты информации связаны применением инструментов шифрования?

а) Организационные средства
б) Аппаратно-программные
в) Криптографические средства

10. К каким средствам защиты информации относятся мероприятия, регламентирующие поведение сотрудника организации?

а) Организационные средства
б) Аппаратно-программные
в) Криптографические средства

Ключ к тесту

№ п/п	Вариант 1	Вариант 2
1	в	а
2	а	а
3	с	в
4	а	с
5	с	в
6	а	а
7	в	с
8	с	а
9	а	с
10	в	а

3. Тематика практических работ:

Практическая работа № 4.

Расчет наводок в каналах связи.

Цель работы: освоение приемов и методов расчета наводок в каналах связи.

Практическая работа № 5.

Побочные электромагнитные излучения ПК. Заземление технических средств и подавление информационных сигналов в цепях заземления.

Цель работы: освоение приемов определения побочных электромагнитных излучений ПК, заземления технических средств и подавления информационных сигналов в цепях заземления.

Практическая работа № 6.

Восстановление информации при перехвате побочных электромагнитных излучений и наводок (ПЭМИН). Комплексы измерения ПЭМИН.

Цель работы: освоение приемов восстановления информации при перехвате побочных электромагнитных излучений и наводок (ПЭМИН), использования комплексов измерения ПЭМИН.

Практическая работа № 7.

Съем информации по электрическим каналам утечки информации.

Цель работы: освоение приемов съема информации по электрическим каналам утечки информации.

Тема 3.2. Физические процессы при подавлении опасных сигналов

1. Перечень вопросов для устного или письменного опроса по теме:

1. Скрытие речевой информации в каналах связи.
2. Подавление опасных сигналов акустоэлектрических преобразований.
3. Экранирование.
4. Зашумление.

2. Тематика практических работ:

Практическая работа № 8.

Организация мероприятий по скрытию речевой информации.

Цель работы: освоение приемов организации мероприятий по скрытию речевой информации.

Раздел 4. Системы защиты от утечки информации

Тема 4.1. Системы защиты от утечки информации по акустическому каналу

1. Перечень вопросов для устного или письменного опроса по теме:

1. Технические средства акустической разведки.
2. Непосредственное подслушивание звуковой информации.
3. Прослушивание информации направленными микрофонами.
4. Система защиты от утечки по акустическому каналу.
5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.

2. Тематика практических работ:

Практическая работа № 9.

Защита от утечки по акустическому каналу.

Цель работы: освоение приемов защиты от утечки по акустическому каналу.

Тема 4.2. Системы защиты от утечки информации по проводному каналу

1. Перечень вопросов для устного или письменного опроса по теме:

1. Принцип работы микрофона и телефона.
2. Использование коммуникаций в качестве соединительных проводов.
3. Негласная запись информации на диктофоны.
4. Системы защиты от диктофонов.
5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.

2. Тематика практических работ:

Практическая работа № 10.

Осуществление акустического контроля источников звуков с помощью направленных микрофонов. Сравнение и оценка направленных микрофонов.

Цель работы: освоение приемов осуществления акустического контроля источников звуков с помощью направленных микрофонов, выполнение сравнения и оценки направленных микрофонов.

Практическая работа № 11.

Организация применения направленных микрофонов на открытой местности, в помещениях.

Цель работы: освоение приемов организации применения направленных микрофонов на открытой местности, в помещениях.

Практическая работа № 12.

Выбор типа микрофона и места его установки. Организация сеанса деловой звукозаписи.

Цель работы: освоение приемов выбора типа микрофона и места его установки, организации сеанса деловой звукозаписи.

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу

1. Перечень вопросов для устного или письменного опроса по теме:

1. Электронные стетоскопы.
2. Лазерные системы подслушивания.
3. Гидроакустические преобразователи.
4. Системы защиты информации от утечки по вибрационному каналу.
5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.

2. Тематика практических работ:

Практическая работа № 13.

Защита от утечки по виброакустическому каналу.

Цель работы: освоение приемов защиты от утечки по виброакустическому каналу

Практическая работа № 14.

Оценка защищенности ограждающих конструкций от утечки информации по виброакустичекому каналу.

Цель работы: освоение приемов оценки защищенности ограждающих конструкций от утечки информации по виброакустичекому каналу.

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу

1. Перечень вопросов для устного или письменного опроса по теме:

1. Прослушивание информации от радиотелефонов.
2. Прослушивание информации от работающей аппаратуры.
3. Прослушивание информации от радиозакладок.
4. Приемники информации с радиозакладок.
5. Прослушивание информации о пассивных закладках.
6. Системы защиты от утечки по электромагнитному каналу.
7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.

2. Тематика практических работ:

Практическая работа № 15.

Определение каналов утечки ПЭМИН.

Цель работы: освоение приемов определения каналов утечки ПЭМИН.

Практическая работа №16.
Защита от утечки по цепям электропитания и заземления.
Цель работы: освоение приемов защиты от утечки по цепям электропитания и заземления.
Практическая работа №17.
Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении.
Цель работы: освоение приемов статистического анализа загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении.

Тема 4.5. Системы защиты от утечки информации по телефонному каналу
1. Перечень вопросов для устного или письменного опроса по теме:
Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
Использование микрофона телефонного аппарата при положенной телефонной трубке.
Утечка информации по сотовым цепям связи.
Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
2. Тематика практических работ:
Практическая работа № 18.
Защита от утечки информации по телефонному каналу.
Цель работы: освоение приемов и методов защиты от утечки информации по телефонному каналу.
Практическая работа № 19.
Оценка защищенности телефонных каналов.
Цель работы: освоение приемов оценки защищенности телефонных каналов.

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу
Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.
Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
2. Тематика практических работ:
Практическая работа № 20.
Организация защиты информации от несанкционированной утечки по электросетевому каналу.
Цель работы: освоение приемов организации защиты информации от несанкционированной утечки по электросетевому каналу.
Практическая работа № 21.
Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств.
Цель работы: освоение приемов оценки защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств.
Практическая работа № 22.
Организация защиты информации от несанкционированной утечки по электросетевому каналу.

Цель работы: освоение приемов организации защиты информации от несанкционированной утечки по электросетевому каналу.

Тема 4.7. Системы защиты от утечки информации по оптическому каналу

1. Перечень вопросов для устного или письменного опроса по теме:

Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.

2. Тематика практических работ:

Практическая работа № 23.

Организация защиты информации по оптическому каналу.

Цель работы: освоение приемов организации защиты информации по оптическому каналу.

Раздел 5. Применение и эксплуатация технических средств защиты информации

Тема 5.1. Применение технических средств защиты информации

1. Самостоятельная работа

1. Технические средства для уничтожения информации и носителей информации, порядок применения.

2. Перечень вопросов для устного или письменного опроса по теме:

1. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.
2. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.
3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

3. Тематика практических работ:

Практическая работа № 24.

Организация защиты информации в условиях применения мобильных устройств обработки и передачи данных.

Практическая работа № 25.

Измерение параметров побочных электромагнитных излучений и наводок при проведении аттестации объектов.

Цель работы: освоение приемов измерения параметров побочных электромагнитных излучений и наводок при проведении аттестации объектов.

Практическая работа № 26.

Проведение испытаний защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами.

Цель работы: освоение приемов проведения испытаний защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами.

Практическая работа № 27.

Проведение измерений параметров фоновых шумов при использовании технических средств защиты информации.

Цель работы: освоение приемов проведения измерений параметров фоновых шумов при использовании технических средств защиты информации.

Практическая работа № 28.
Организация технического контроля эффективности мер защиты информации.
Цель работы: освоение приемов организации технического контроля эффективности мер защиты информации.

Тема 5.2. Эксплуатация технических средств защиты информации
1. Самостоятельная работа
1. Этапы эксплуатации технических средств защиты информации.
2. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.

2. Перечень вопросов для устного или письменного опроса по теме:
1. Установка и настройка технических средств защиты информации.
2. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
3. Организация ремонта технических средств защиты информации.
4. Проведение аттестации объектов информатизации.

3. Тематика практических работ:
Практическая работа № 29.
Проведение технического обслуживания телефонных аппаратов.
Цель работы: освоение приемов проведения технического обслуживания телефонных аппаратов.
Практическая работа № 30.
Проведение технического обслуживания шредеров.
Цель работы: освоение приемов проведение технического обслуживания шредеров.
Практическая работа № 31.
Проведение первичного осмотра помещений при аттестации объекта информатизации.
Цель работы: освоение приемов проведения первичного осмотра помещений при аттестации объекта информатизации.
Практическая работа № 32.
Проведение оценки разведдоступности.
Цель работы: освоение приемов проведения оценки разведдоступности.
Практическая работа № 33.
Комплекс работ по проверке возможности утечки информации по техническим каналам.
Цель работы: освоение приемов проведения комплекса работ по проверке возможности утечки информации по техническим каналам.
Практическая работа № 34.
Оценка защищенности объекта информатизации.
Цель работы: освоение приемов оценки защищенности объекта информатизации.
Практическая работа № 35.
Подготовка пакета документов для проведения аттестации объекта информатизации.
Цель работы: освоение приемов подготовки пакета документов для проведения аттестации объекта информатизации.

Критерии оценок устных вопросов:

Оценка «Отлично» ставится, если дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;

доказательно раскрыты основные понятия, термины и др.; в ответе отслеживается четкая структура, выстроенная в логической последовательности; ответ изложен грамотным языком; на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

Оценка «Хорошо» ставится, если дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала; ответ четко структурирован, выстроен в логической последовательности; изложен грамотным языком; однако были допущены неточности в определении понятий, терминов

Оценка «Удовлетворительно» ставится, если дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют некоторые нарушения; допущены несущественные ошибки в изложении теоретического материала и употреблении терминов; знания показаны слабо, речь неграмотная.

Оценка «Неудовлетворительно» ставится, если дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения; допущены существенные ошибки в теоретическом материале (понятиях, терминах); знания отсутствуют, речь неграмотная.

3.2. Типовые задания для промежуточного контроля по МДК.03.01 Техническая защита информации

Вопросы к экзамену

1. Понятие информации. Проблема обеспечения безопасности в информационных системах, политика информационной безопасности.
2. Устройства защиты от утечки информации по радиоканалам, основные методы обнаружения радиозакладок.
3. Физические средства
4. Аппаратные средства
5. Программные средства
6. Криптографические средства
7. Индикаторы поля, акустическая развязка, дифференциальный индикатор поля.
8. Генераторы шума.
9. Особенности работы и основные характеристики сканирующих радиоприемников.
10. Блок-схема типового сканирующего радиоприемника.
11. Автоматизированные комплексы обнаружения радиозакладок. Методы обнаружения локализации в пространстве закладных устройств.
12. Виды модуляции и кодирования передаваемой информации.
13. Амплитудная модуляция. Амплитудная модуляция с подавлением верхней или нижней боковой частоты. Частотная модуляция. Фазовая модуляция.
14. Кодово-импульсная модуляция. Специальные виды модуляции. Основные требования к специальным системам связи.
15. Использование ШПС и ППРЧ сигналов. Основные характеристики.
16. Обнаружители и подавители диктофонов. Назначение. Принципы работы. Основные характеристики.
17. Принципы работы локаторов нелинейностей. Основные методы обнаружения ложных и истинных соединений.
18. Концепции инженерно-технической защиты информации.
19. Системный подход к защите информации.

20. Основные проблемы инженерно-технической защиты информации.
21. Основные концептуальные положения инженерно-технической защиты информации.
22. Направления инженерно-технической защиты информации.
23. Показатели эффективности инженерно-технической защиты информации.
24. Теоретические основы инженерно-технической защиты информации.
25. Источники опасных сигналов.
26. Виды побочных опасных электромагнитных излучений.
27. Характеристика технической разведки.
28. Технические каналы утечки информации.
29. Методы инженерно-технической защиты информации.
30. Методы инженерной защиты и технической охраны объекта.
31. Методы скрытия информации и ее носителей.
32. Физические основы защиты информации.
33. Физические основы побочных электромагнитных излучений и наводок.
34. Распространение сигналов в технических каналах утечки информации.
35. Физические процессы подавления опасных сигналов.
36. Технические средства добывания и инженерно-технической защиты.
37. Средства технической разведки.
38. Средства инженерной защиты и технической охраны.
39. Средства предотвращения утечки информации по техническим каналам.
40. Организационные основы инженерно-технической защиты информации.
41. Государственная система защиты информации.
42. Контроль эффективности инженерно-технической защиты информации.
43. Методическое обеспечение инженерно-технической защиты автоматизированных систем от вредоносных программных воздействий.
44. Моделирование инженерно-технической защиты информации.
45. Методические рекомендации оценки эффективности защиты информации.

Критерии оценок:

Оценка «отлично», если студент обладает глубокими и прочными знаниями программного материала; при ответе на вопросы продемонстрировал исчерпывающее, последовательное и логически стройное изложение; правильно сформулировал понятия и закономерности по вопросам; сделал вывод по излагаемому материалу;

Оценка «хорошо», если студент обладает достаточно полным знанием программного материала; его ответ представляет грамотное изложение учебного материала; но имеются существенные неточности в формулировании понятий и закономерностей по вопросам; не полностью сделаны выводы по излагаемому материалу;

Оценка «удовлетворительно», если студент имеет общие знания основного материала без усвоения некоторых существенных положений; формулирует основные понятия с некоторой неточностью; затрудняется в приведении примеров, подтверждающих теоретические положения;

Оценка «неудовлетворительно», если студент не знает значительную часть программного материала; допустил существенные ошибки в процессе изложения; не умеет выделить главное и сделать вывод; приводит ошибочные определения; ни один вопрос не рассмотрен до конца, наводящие вопросы не помогают.

3.3. Типовые задания для текущего контроля по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Тема 1.1. Цели и задачи физической защиты объектов информатизации

1. Перечень вопросов для устного или письменного опроса по теме:

1. Предмет и задачи технической защиты информации.
2. Системный подход при решении задач инженерно-технической защиты объектов.
3. Задачи и требования к способам и средствам защиты информации техническими средствами.
4. Характеристики потенциально опасных объектов.
5. Содержание и задачи физической защиты объектов информатизации.
6. Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект.
7. Особенности задач охраны различных типов объектов.

2. Самостоятельная работа

1. Основные понятия инженерно-технических средств физической защиты.
2. Категорирование объектов информатизации.

3. Тематика практических работ:

Практическая работа № 1.

Построение модели нарушителя, определение способов его проникновения на объект, на примере образовательной организации.

Цель работы: освоение приемов построения модели нарушителя, определения способов его проникновения на объект на примере образовательной организации.

Практическая работа № 2.

Построение модели нарушителя, определение способов его проникновения на объект, на примере производственной организации.

Цель работы: освоение приемов построения модели нарушителя, определения способов его проникновения на объект, на примере производственной организации.

Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты

1. Перечень вопросов для устного или письменного опроса по теме:

1. Общие принципы обеспечения безопасности объектов.
2. Жизненный цикл системы физической защиты.
3. Принципы построения интегрированных систем охраны.
4. Классификация и состав интегрированных систем охраны.
5. Требования к инженерным средствам физической защиты.
6. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
7. Типовой вариант КПП.
8. Быстро развертываемые комплексы ТСО: состав, отличительные особенности, преимущества от внедрения.

2. Тематика практических работ:

Практическая работа № 3.

Формирование требований к физической защите объекта. Анализ нормативно-правовых документов.

Цель работы: освоение приемов формирования требований к физической защите объекта, анализа нормативно-правовых документов.

Практическая работа № 4.

Формирование перечня требований к защите объекта.

Цель работы: освоение приемов формирования перечня требований к защите объекта.

Практическая работа № 5.

Определение состава инженерных конструкций, необходимых для предотвращения проникновения злоумышленника.

Цель работы: освоение приемов определения состава инженерных конструкций, необходимых для предотвращения проникновения злоумышленника.

Практическая работа № 6.

Разработка проекта монтажа инженерных конструкций на территории организации.

Цель работы: освоение приемов разработки проекта монтажа инженерных конструкций на территории организации.

Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

1. Перечень вопросов для устного или письменного опроса по теме:

1. Информационные основы построения системы охранной сигнализации.
2. Назначение, классификация технических средств обнаружения.
3. Построение систем обеспечения безопасности объекта.
4. Периметровые средства обнаружения: назначение, устройство, принцип действия.
5. Объектовые средства обнаружения: назначение, устройство, принцип действия.
6. Номенклатура применяемых средств обнаружения (вибрационные, магнитометрические, объектовые).
7. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД.
8. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.
9. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.
10. Обнаружение металлических предметов и радиоактивных веществ.

2. Тематика практических работ:

Практическая работа № 7.

Монтаж датчиков пожарной сигнализации.

Цель работы: освоение приемов монтажа датчиков пожарной сигнализации.

Практическая работа № 8.

Монтаж датчиков охранной сигнализации.

Цель работы: освоение приемов монтажа датчиков охранной сигнализации.

Тема 2.2. Система контроля и управления доступом

1. Перечень вопросов для устного или письменного опроса по теме:

1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.
2. Особенности построения и размещения СКУД.
3. Структура и состав СКУД.
4. Периферийное оборудование и носители информации в СКУД.
5. Основы построения и принципы функционирования СКУД.
6. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.
7. Обнаружение металлических предметов и радиоактивных веществ.

2. Тематика практических работ:

Практическая работа № 9.

Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя.

Цель работы: освоение приемов рассмотрения принципов устройства, работы и применения аппаратных средств аутентификации пользователя.

Практическая работа № 10.

Рассмотрение принципов устройства, работы и применения средств контроля доступа.

Цель работы: освоение приемов рассмотрения принципов устройства, работы и применения средств контроля доступа.

Практическая работа № 11.

Особенности построения и размещения СКУД.

Цель работы: освоение приемов определения особенности построения и размещения СКУД.

Практическая работа № 12.

Периферийное оборудование и носители информации в СКУД. Методы удостоверения личности, применяемые в СКУД.

Цель работы: освоение приемов работы с периферийным оборудованием и носителями информации в СКУД, методов удостоверения личности, применяемые в СКУД.

Практическая работа № 13.

Сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза.

Цель работы: освоение приемов сравнительного анализа применения шлюзового турникета и маятниковой двери-шлюза.

Тема 2.3. Система телевизионного наблюдения

1. Самостоятельная работа

1. Аналоговые и цифровые системы видеонаблюдения.
2. Назначение системы телевизионного наблюдения.

2. Перечень вопросов для устного или письменного опроса по теме:

1. Состав системы телевизионного наблюдения.
2. Видеокамеры.
3. Объективы.
4. Термокожухи.
5. Поворотные системы.
6. Состав системы телевизионного наблюдения.
7. Инфракрасные осветители.
8. Детекторы движения.

9. Дополнительное оборудование систем телевизионного наблюдения

3. Тематика практических работ:

Практическая работа № 14.

Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.

Цель работы: освоение приемов рассмотрения принципов устройства, работы и применения средств видеонаблюдения.

Практическая работа № 15.

Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.

Цель работы: освоение приемов рассмотрения принципов работы системы видеонаблюдения и ее проектирование.

Практическая работа № 16.

Управление системой телевизионного наблюдения с автоматизированного рабочего места.

Цель работы: освоение приемов управления системой телевизионного наблюдения с автоматизированного рабочего места.

Практическая работа № 17.

Разработка проекта системы видеонаблюдения для организации.

Цель работы: освоение приемов разработки проекта системы видеонаблюдения для организации.

Практическая работа № 18.

Настройка систем телевизионного наблюдения с учетом специфики деятельности организации.

Цель работы: освоение приемов настройки систем телевизионного наблюдения с учетом специфики деятельности организации.

Тема 2.4. Система сбора, обработки, отображения и документирования информации

1. Перечень вопросов для устного или письменного опроса по теме:

1. Классификация системы сбора и обработки информации.
2. Схема функционирования системы сбора и обработки информации.
3. Варианты структур построения системы сбора и обработки информации.
4. Устройства отображения и документирования информации.

2. Тематика практических работ:

Практическая работа № 19.

Рассмотрение принципов устройства системы сбора и обработки информации.

Цель работы: освоение приемов рассмотрения принципов устройства системы сбора и обработки информации.

Практическая работа № 20.

Рассмотрение принципов работы и применения системы сбора и обработки информации.

Цель работы: освоение приемов рассмотрения принципов работы и применения системы сбора и обработки информации.

Практическая работа № 21.

Практическое исследование особенностей применения систем сбора, обработки, отображения и документирования информации.

Цель работы: освоение приемов практического исследования особенностей применения систем сбора, обработки, отображения и документирования информации.

Практическая работа № 22.

Определение состава ССОИ для образовательной организации.

Цель работы: освоение приемов определения состава ССОИ для образовательной организации.

Тема 2.5 Система воздействия

1. Перечень вопросов для устного или письменного опроса по теме:

1. Назначение и классификация технических средств воздействия.
2. Основные показатели технических средств воздействия.
3. Организация охраны объектов с применением технических средств воздействия.

2. Тематика практических работ:

Практическая работа № 23.

Мониторинг эффективности технических средств воздействия для гражданских организаций.

Цель работы: освоение приемов мониторинга эффективности технических средств воздействия для гражданских организаций.

Практическая работа № 24.

Определение эффективности технических средств воздействия для гражданских организаций.

Цель работы: освоение приемов определения эффективности технических средств воздействия для гражданских организаций.

Практическая работа № 25.

Испытание на устойчивость технических средств охраны.

Цель работы: освоение приемов испытания на устойчивость технических средств охраны.

Практическая работа № 26.

Разработка проекта применения технических средств воздействия для образовательной организации.

Цель работы: освоение приемов разработки проекта применения технических средств воздействия для образовательной организации.

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты

Тема 3.1 Применение инженерно-технических средств физической защиты

1. Самостоятельная работа

Нормативная документация использования технических средств физической защиты. Единая система конструкторской документации. Единая система технологической документации. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.

2. Перечень вопросов для устного или письменного опроса по теме:

1. Периметровые и объектовые средства обнаружения, порядок применения.
2. Работа с периферийным оборудованием системы контроля и управления доступом.
3. Особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов.
4. Особенности монтажа.
5. Особенности организации пропускного режима на КПП.
6. Управление системой телевизионного наблюдения с автоматизированного рабочего места.

3. Тематика практических работ:

Практическая работа № 27.
Разработка структурной схемы оборудования инженерно-технических средств физической защиты.
Цель работы: освоение приемов разработки структурной схемы оборудования инженерно-технических средств физической защиты.
Практическая работа № 28.
Представление моделей объектов информационной безопасности.
Цель работы: освоение приемов представления моделей объектов информационной безопасности.
Практическая работа № 29.
Разработка спецификации оборудования физической защиты объекта.
Цель работы: освоение приемов разработки спецификации оборудования физической защиты объекта.
Практическая работа № 30.
Определение эффективности применения сигнально-охранных пиротехнических устройств для гражданских организаций.
Цель работы: освоение приемов определения эффективности применения сигнально-охранных пиротехнических устройств для гражданских организаций.

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты
1. Самостоятельная работа
1. Этапы эксплуатации.
2. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.

2. Перечень вопросов для устного или письменного опроса по теме:
1. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.
2. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.
3. Организация ремонта технических средств физической защиты.

3. Тематика практических работ:
Практическая работа № 31.
Проведение диагностики систем видеонаблюдения.
Цель работы: освоение приемов проведения диагностики систем видеонаблюдения.
Практическая работа № 32.
Устранение отказов и восстановление работоспособности систем видеонаблюдения.
Цель работы: освоение приемов устранения отказов и восстановления работоспособности систем видеонаблюдения.
Практическая работа № 33.
Отработка конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД.
Цель работы: освоение приемов отработки конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД.
Практическая работа № 34.
Проверка работоспособности средств защиты информации от несанкционированного доступа и специальных воздействий.

Цель работы: освоение приемов проведения проверки работоспособности средств защиты информации от несанкционированного доступа и специальных воздействий.

Практическая работа № 35.

Выполнение правил эксплуатации средств защиты информации.

Цель работы: освоение приемов выполнения правил эксплуатации средств защиты информации.

3.4. Тематика курсовых работ по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Курсовая работа должна быть оформлена соответствующим образом, согласно методическим рекомендациям. В противном случае она не принимается преподавателем к оцениванию.

Тематика курсового проекта (работы):

1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации.
2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.
3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.
4. Разработка проекта системы контроля и управления доступом служебного офиса.
5. Разработка проекта системы обеспечения безопасности для торговой организации.
6. Разработка проекта системы обеспечения безопасности для образовательной организации.
7. Разработка проекта системы обеспечения безопасности для промышленного предприятия.
8. Разработка проекта системы обеспечения безопасности для банковской организации.
9. Разработка проекта КПП для гражданской организации.
10. Разработка проекта систем телевизионного наблюдения для образовательной организации.
11. Разработка мероприятий применения пассивных методов защиты акустической информации.
12. Разработка мероприятий применения активных методов защиты акустической информации.
13. Подготовка пакета документов для проведения аттестации объекта информатизации на примере организации.
14. Разработка требований к инженерно-техническим средствам для физической защиты автоматизированных рабочих мест на объекте.
15. Разработка требований по защите информации от несанкционированного доступа к объекту информатизации.
16. Использование комплексного обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему.
17. Реализация комплексного подхода к обеспечению защиты конфиденциальной информации в компании.
18. Разработка концепции политики безопасности и систем контроля доступа для локальной вычислительной сети.

19. Организация порядка установления внутри объектного спец режима на объекте информатизации.
20. Организация противодействия угрозам безопасности персонала организации.
21. Разработка основных направлений, принципов и методов обеспечения информационной безопасности предприятия.
22. Построение типовой модели угроз безопасности информации кредитной организации.
23. Разработка комплексной системы защиты коммерческой информации на предприятии.
24. Разработка мер по технической защите конфиденциальной информации в организации.
25. Разработка мер информационной безопасности предприятия.
26. Реализация комплексного подхода к обеспечению защиты конфиденциальной информации в компании.
27. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.
28. Разработка структуры службы безопасности предприятия.
29. Разработка рабочего проекта охранной безопасности на предприятии.
Инженерно-технические средства обеспечения безопасности предприятия.

3.5. Тематика курсовых работ по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Вопросы к дифференцированному зачету:

1. Инженерно-техническая защита
2. Физические средства
3. Аппаратные средства
4. Программные средства
5. Криптографические средства
6. ПК на предмет определения максимального расстояния, при котором информацию можно снять с ПК, физически не подключаясь к нему;
7. Оценивается система видеонаблюдения помещения, где расположен сервер;
8. Проверяются помещения, предназначенные для переговоров, на предмет наличия различных подслушивающих устройств;
9. Производится установка специального оборудования, призванного распознавать подслушивающие устройства
10. Утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности
11. Детекторы, индикаторы поля и тест-приёмники;
12. Анализаторы проводных коммуникаций;
13. Многофункциональные поисковые приборы;
14. Обнаружители скрытых видеокамер;
15. Нелинейные локаторы;
16. Комплексы радиомониторинга и пеленгования;
17. Средства защиты от утечки акустической информации;
18. Устройства противодействия радиоэлектронным средствам негласной аудиозаписи;
19. Устройства блокирования работы систем проводной, мобильной связи и передачи данных;
20. Устройства защиты от прослушивания телефонных переговоров;

21. Устройства защиты от утечки информации по цепям электропитания (фильтры помехоподавляющие электрические) и заземления;
22. Устройства защиты от утечки информации по каналам ПЭМИН;
23. Устройства хранения, копирования, уничтожения и восстановления информации;
24. Цифровые системы регистрации, звукозаписи и шумоочистки речевых сигналов;
25. Металлодетекторы ручные досмотровые;
26. Металлоискатели поисковые грунтовые, глубинные;
27. Металлодетекторы арочные стационарные досмотровые;
28. Программных средств сбора, анализа и обработки информации;
29. Радиоэкранирующих и радиопоглощающих материалов шумопоглощающих материалов.
30. Комплексное использование технических, программных и организационных средств
31. Информация как объект защиты
32. Требования к защищенности информации
33. Организационные меры защиты информации
34. Оценка вероятного противника
35. Оценка условий решения задачи защиты информации
36. Инженерно-технические меры защиты информации
37. Системы информационной безопасности
38. Принципы построения систем безопасности
39. Защита компьютерной информации
40. Угрозы несанкционированного доступа в сеть
41. Системы информационной безопасности сети
42. Принципы построения систем безопасности сети
43. Аппаратные средства защиты передаваемых данных
44. Разработка системы управления объектом защиты и безопасности
45. Постановка задачи проектирования
46. Анализ объекта защиты
47. Контролируемая зона
48. Возможные каналы утечки информации
49. Разработка политики защиты контролируемой зоны
50. Обеспечение защиты помещения проведения совещаний
51. Обеспечение защиты помещения руководителя
52. Обеспечение защиты помещения серверной
53. Разработка политики безопасности сети и коммуникаций
54. Интернет-шлюз + файерволл как основа системы управления
55. Выбор и конфигурирование аппаратных средств защиты данных
56. Защита данных средствами защиты информации и специального ПО
57. Описание настройки специального программного обеспечения защиты данных
58. Моделирование объектов защиты.

3.6. Типовые задания для текущего контроля по МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности

Раздел 1. Защита информации от внутренних угроз информационной безопасности с использованием DLP-технологий

Тема 1.1. Основы защиты информации от внутренних угроз информационной безопасности.

1. Перечень вопросов для устного или письменного опроса по теме:

1. Основы защиты корпоративной информации.
2. Цели, задачи, методы и средства защиты информации.
3. Защита информации от внутренних угроз информационной безопасности.
4. Выявление утечек с использованием технологии Data Leakage Prevention (DLP).
5. Теория и практика применения DLP систем.
6. Назначение системы Info Watch Traffic Monitor (IW TM).
7. Контролируемые каналы передачи данных.
8. Архитектура продукта IW TM.
9. Технологии анализа детектируемых объектов.
10. Задачи и принципы работы дополнительных модулей системы IW Device Monitor (IW DM) и IW Crawler.
11. Визуальная аналитика данных.

2. Самостоятельная работа

1. Правовые основы защиты корпоративной информации.
2. Ключевые алгоритмы и системы.
3. Основные понятия.
4. Безопасность информационных систем.
5. Угрозы информационной безопасности.
6. Уязвимости.
7. Риски.
8. Атаки.

Тема 1.2. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

1. Перечень вопросов для устного или письменного опроса по теме:

1. Сетевое окружение.
2. Сетевые протоколы.
3. Методы выявления и построения путей движения информации в организации.
4. Подходы к построению сети.
5. Настройка сетевых устройств для эффективного взаимодействия.
6. Типы сетевых устройств.
7. Разнообразие операционных систем, их возможности с точки зрения использования и развертывания компонент систем защиты от внутренних угроз.
8. Процесс выбора драйверов и программного обеспечения для различных аппаратных средств и операционных систем.
9. Технологии программной и аппаратной виртуализации.
10. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин, и т.п.
11. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развертывании и настройке.
12. Установка и настройка агентского мониторинга.

13. Синхронизация с LDAPсервером.

2. Самостоятельная работа

1. Этапы установки систем корпоративной защиты от внутренних угроз.
2. Назначение компонент системы корпоративной защиты от внутренних угроз.

3. Тематика практических работ:

Практическая работа № 1.

Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.

Цель работы: освоение приемов

Практическая работа № 2.

Установка сервера Traffic Monitor.

Цель работы: освоение приемов установки сервера Traffic Monitor.

Практическая работа № 3.

Установка лицензии Traffic Monitor. Установка Базы данных.

Цель работы: освоение приемов установки лицензии Traffic Monitor, Базы данных.

Практическая работа № 4

Установка подсистемы Краулер. Установка рабочего места Офицера Безопасности. Создание пользователя виртуальной машины IWDM (Офицер Безопасности). Настройка рабочего места Офицера Безопасности. Конфигурация сетевой инфраструктуры: настройка хост машины, сетевого окружения, виртуальных машин.

Цель работы: освоение приемов установки подсистемы Краулер, установки и настройки рабочего места Офицера Безопасности.

Практическая работа № 5.

Установка серверной части Info Watch Device Monitor. Установка рабочего места потенциального нарушителя. Настройка сетевого взаимодействия. Создание пользователя виртуальной машины Agent1 (Потенциальный нарушитель). Настройка рабочего места на машине Agent1. Установка DM Client.

Цель работы: освоение приемов установки серверной части Info Watch Device Monito, рабочего места потенциального нарушителя.

Практическая работа № 6.

Работа в Консоли управления Device Monitor. Авторизация и соединение с сервером InfoWatch Device Monitor. Главное окно Консоли управления (DM). Разделы Консоли управления (DM).

Цель работы: освоение приемов установки серверной части Info Watch Device Monitor, рабочего места потенциального нарушителя.

Тема 1.3. Исследование (аудит) организации с целью защиты от внутренних угроз

1. Перечень вопросов для устного или письменного опроса по теме:

Угрозы информационной безопасности. Исследование (аудит) организации на основании полученных материалов («модели организации»), обследование корпоративных информационных систем.

Определение объектов защиты. Перечень субъектов, персон, роли пользователей, права доступа.

2. Тематика практических работ:

Практическая работа № 7.

Изучение структуры организации. Обследование корпоративных информационных систем.

Цель работы: освоение приемов изучения структуры организации, обследования корпоративных информационных систем.

Практическая работа № 8.

Добавление роли Администратора системы. Добавление роли пользователя для проведения аудита.

Цель работы: освоение приемов добавления роли Администратора системы, добавления роли пользователя для проведения аудита.

Практическая работа № 9.

Создание подразделений организации с использованием AD сервера. Синхронизация каталога пользователей и компьютеров.

Цель работы: освоение приемов создания подразделений организации с использованием AD сервера, синхронизации каталога пользователей и компьютеров.

Тема 1.4. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

1. Перечень вопросов для устного или письменного опроса по теме:

1. Работа с интерфейсом управления системы корпоративной защиты информации.
2. Раздел Технологии.
3. Работа с объектами защиты в интерфейсе управление системой.
4. Политика безопасности. Модификация политики безопасности в системе IWTM.

2. Тематика практических работ:

Практическая работа № 10.

Работа с категориями и терминами.

Цель работы: освоение приемов работы с категориями и терминами.

Практическая работа № 11.

Работа с текстовыми объектами.

Цель работы: освоение приемов работы с текстовыми объектами.

Практическая работа № 12.

Работа с эталонными документами.

Цель работы: освоение приемов работы с эталонными документами.

Практическая работа № 13.

Работа с бланками.

Цель работы: освоение приемов работы с бланками.

Практическая работа № 14.

Работа с печатями.

Цель работы: освоение приемов работы с печатями.

Практическая работа № 15.

Работа с выгрузками.

Цель работы: освоение приемов работы с выгрузками.

Практическая работа № 16.

Работа с графическими объектами.

Цель работы: освоение приемов работы с графическими объектами.

Практическая работа № 17.

Экспорт и импорт базы технологий.

Цель работы: освоение приемов экспорта и импорта базы технологий.

Практическая работа № 18.

Работа с объектами защиты. Создание каталога объектов защиты. Создание объекта защиты.
Цель работы: освоение приемов работы с объектами защиты, создания каталога объектов защиты, создания объекта защиты.

Практическая работа № 19.

Добавление элементов технологий. добавление условий обнаружения. Создание политики для объектов защиты и их каталогов.

Цель работы: освоение приемов добавления элементов технологий, добавления условий обнаружения, создания политики для объектов защиты и их каталогов.

Практическая работа № 20.

Добавление новой политики: создание политики защиты данных, создание политики защиты данных на агентах, создание политики контроля персон.

Цель работы: освоение приемов добавления новой политики: создания политики защиты данных, создания политики защиты данных на агентах, создания политики контроля персон.

Практическая работа № 21.

Добавление правил в политику. Фильтрация списка политик.

Цель работы: освоение приемов добавления правил в политику, фильтрации списка политик.

Тема 1.5. Технологии агентского мониторинга

1. Перечень вопросов для устного или письменного опроса по теме:

1. Состав серверной части InfoWatch Device Monitor: база данных, сервер InfoWatch Device Monitor, консоль управления InfoWatch Device Monitor.
2. Общие принципы работы с Консолью управления InfoWatch Device Monitor (DM): авторизация и соединение с сервером InfoWatch Device Monitor, главное окно Консоли управления, разделы Консоли управления.
3. Управление схемой безопасности.
4. Организация схемы безопасности.
5. Политики безопасности и правила (DM).
6. Сотрудники и группы сотрудников.
7. Компьютеры и группы компьютеров.
8. Загрузка схемы безопасности на контролируемые компьютеры.
9. Общие действия при управлении схемой безопасности.
10. Просмотр действующей версии схемы безопасности.
11. Редактирование и обновление схемы безопасности.
12. Экспорт/импорт конфигурации.
13. Настройка схемы безопасности.
14. Политики безопасности (DM).
15. Просмотр политик безопасности (DM).
16. Создание и настройка политики безопасности (DM).
17. Редактирование политики безопасности (DM).
18. Удаление политики безопасности (DM).
19. Правила (DM).
20. Применение правил (DM).
21. Типы правил.
22. Создание, редактирование, копирование и удаление правил (DM).
23. Удаленная установка, обновление и удаление Агентов. Управление задачами в Консоли управления DM.

24. Просмотр событий DM. Фильтры событий.

2. Самостоятельная работа

1. Способы установки Агента Device Monitor на рабочие станции: Локальная установка, удаленная, через задачи распространения в Консоли управления, установка с помощью средств распространения программного обеспечения.

3. Тематика практических работ:

Практическая работа № 22.

Учетные записи пользователей Консоли управления (DM). Добавление учетной записи Консоли управления. Редактирование учетной записи Консоли управления (DM). Блокирование и разблокирование учетной записи Консоли управления (DM). Удаление учетной записи Консоли управления (DM).

Цель работы: освоение приемов работы с Консолью управления DM.

Практическая работа № 23.

Роли пользователей Консоли управления (DM). Добавление роли пользователя Консоли управления. Редактирование роли пользователя. Удаление роли пользователя.

Цель работы: освоение приемов работы с ролями пользователей Консоли управления (DM).

Практическая работа № 24.

Общие настройки Агентов. Контроль сетевых соединений. Контроль сетевого трафика.

Цель работы: освоение приемов работы с настройками Агентов.

Практическая работа № 25.

Настройки сервера Device Monitor. Соединение с сервером Traffic Monitor. Соединение и синхронизация со службами каталогов.

Цель работы: освоение приемов работы с сервером Traffic Monitor.

Практическая работа № 26.

Настройка уведомлений сотрудников о нарушении правил (DM). Исключение приложений из перехвата.

Цель работы: освоение приемов работы с правилами нарушений.

Практическая работа № 27.

Контроль приложений и снимки экрана. Хранение событий. Синхронизация политик Traffic Monitor. Контроль ввода с клавиатуры.

Цель работы: освоение приемов осуществления контроля приложений Traffic Monitor.

Практическая работа № 28.

Настройка Правила для Application Monitor. Правило для Clipboard Monitor. Правило для Cloud Storage Monitor. Правило для Device Monitor.

Цель работы: освоение приемов настойки правил TM.

Практическая работа № 29.

Правило (DM) для File Monitor. Правило для File Operations Monitor. Правило для FTP Monitor. Правило для HTTP(S) Monitor. Правило для IM Client Monitor.

Цель работы: освоение приемов настройки правил DM.

Практическая работа № 30.

Правило (DM) для Mail Monitor. Правило для Network Monitor. Правило для Print Monitor. Правило для ScreenShot Control Monitor. Правило для ScreenShot Monitor.

Цель работы: освоение приемов работы с правилами TM.

Практическая работа № 31.

Белые списки устройств. Просмотр сведений о белых списках. Добавление белого списка. Установка периода действия записи. Редактирование белого списка. Удаление белого списка.

Цель работы: освоение приемов работы с белыми списками.

Практическая работа № 32.

Приложения. Создание и изменение списка приложений. Добавление приложения в список автоматически. Добавление приложения в список вручную. Экспорт протокола приложения.

Цель работы: освоение приемов работы с приложениями.

Практическая работа № 33.

Временный доступ сотрудника к сети. Временный доступ сотрудника к устройствам.

Цель работы: освоение приемов доступа к сети.

Практическая работа № 34.

Создание задачи первичного распространения. Создание задачи обновления, задачи смены пароля деинсталляции.

Цель работы: освоение приемов создания задач первичного распространения, обновления, смены пароля.

Практическая работа № 35.

Создание задачи удаления. Запуск, остановка, редактирование и удаление задачи.

Цель работы: освоение приемов создания задачи удаления, запуска, остановки, редактирования и удаления задачи.

Практическая работа № 36.

Просмотр событий DM. Фильтры событий. Удаление событий.

Цель работы: освоение приемов просмотра и фильтрации событий.

Тема 1.6. Анализ выявленных инцидентов

1. Перечень вопросов для устного или письменного опроса по теме:

1. Создание тестовой политики в IWTM.
2. Создание тестовой политики в DM.
3. Работа в тематических разделах Сводка, События интерфейса Консоли управления Traffic Monitor.
4. Отчеты интерфейса Консоли управления Traffic Monitor.

2. Тематика практических работ:

Практическая работа № 37.

Создание тестовой политики в IWTM.

Цель работы: освоение приемов создания тестовой политики в IWTM.

Практическая работа № 38.

Создание тестовой политики в DM.

Цель работы: освоение приемов создания тестовой политики в DM.

Практическая работа № 39.

Генерация событий для тестирования политики.

Цель работы: освоение приемов генерации событий для тестирования политики.

Практическая работа № 40.

Работа с отчетами. Создание и просмотр отчетов. Создание папки с отчетами.

Цель работы: освоение приемов работы с отчетами.

Практическая работа № 41.

Создание и настройка виджета. Просмотр готовых отчетов.

Цель работы: освоение приемов с виджетами.

Раздел 2. Технология анализа и защиты сетевого трафика

Тема 2.1. Программные решения построения и управления виртуальными и защищенными сетями

1. Перечень вопросов для устного или письменного опроса по теме:

1. Технология защиты информации VipNet.
2. Структура сети VipNet.
3. Типы связей в сети VipNet.
4. Управляющий драйвер.
5. Виртуальные адреса сети VipNet.
6. Основные компоненты сети VipNet.
7. Базовые модули VipNet.
8. VipNet Администратор.
9. VipNet Координатор.
10. VipNet Клиент.
11. VipNet Policy Manager.

Тема 2.2. Базовый программный комплекс VipNet Administrator

1. Перечень вопросов для устного или письменного опроса по теме:

1. VipNet Центр управления сетью (ЦУС).
2. Основные функциональные возможности.
3. Архитектура программы VipNet ЦУС.
4. Взаимодействие с программой VipNet Удостоверяющий и ключевой центр и с программой VipNet Registration Point.
5. Связи между объектами сети VipNet.
6. Роли сетевых узлов.
7. Справочники и ключи VipNet.
8. Топология сети: основные понятия сетевого уровня.
9. Функции координатора в защищенной сети VipNet.
10. Туннелирование.
11. Принципы осуществления соединений в сети VipNet.
12. Организация межсетевого взаимодействия.
13. VipNet Удостоверяющий и ключевой центр (УКЦ).
14. Основные функции VipNet УКЦ.
15. Программный комплекс VipNet Удостоверяющий центр (УЦ).
16. Инфраструктура открытых ключей KPI.
17. Электронная подпись данных.
18. Шифрование данных.
19. Работа Удостоверяющего центра.
20. Использование центра регистрации.
21. Архитектура KPI.
22. Модели установления доверительных отношений.
23. Программный комплекс VipNet УЦ.
24. Ключевая система в ПО VipNet.
25. Формирование ключевой информации в VipNet.
26. Мастер-ключи.
27. Формирование ключей при первоначальном развертывании сети.
28. Дистрибутивы ключей.

29. Ключи пользователя.
30. Ключи узла.
31. Компрометация ключей.
32. Резервный набор персональных ключей.
33. Межсетевые мастер-ключи.
34. Электронная подпись.
35. Сертификат ключа проверки ЭП.

2. Тематика практических работ:

Практическая работа № 42.

Планирование защищенной сети VipNet. Проработка схемы сети.

Цель работы: освоение приемов планирования защищенной сети.

Практическая работа № 43.

Подготовка виртуального стенда. Создание и настройка виртуальных машин.

Цель работы: освоение приемов создания виртуального стенда.

Практическая работа № 44.

Установка и первичная настройка компонентов программного обеспечения ViPNet Administrator.

Цель работы: освоение приемов первичной настройки ViPNet.

Практическая работа № 45.

Создание структуры защищенной сети.

Цель работы: освоение приемов создания структуры защищенной сети.

Практическая работа № 46.

Создание межсерверных каналов и связей.

Цель работы: освоение приемов создания межсерверных каналов.

Практическая работа № 47.

Первый запуск программы ViPNet Удостоверяющий и ключевой центр. Выдача дистрибутивов ключей.

Цель работы: освоение приемов запуска ViPNet, выдачи дистрибутивов ключей.

Практическая работа № 48.

Настройка резервного копирования и восстановление данных в ПО ViPNet Administrator.

Цель работы: освоение приемов резервного копирования и восстановления данных.

Тема 2.3. Программное обеспечение ViPNet Client

1. Перечень вопросов для устного или письменного опроса по теме:

Назначение ПО ViPNet Client. Функции ПО ViPNet Client. Состав ПО ViPNet Client. Драйвер сетевой защиты.

Программа VipNet Монитор. Основные принципы фильтрации трафика. Обмен защищенными сообщениями. Конференция. Файловый обмен. вызов внешних приложений. Просмотр веб-ресурсов сетевого узла.

Транспортный модуль VipNet MFTP. Контроль приложений VipNet. Деловая почта VipNet. Криптопровайдер VipNet CSP. Система обновления VipNet.

2. Тематика практических работ:

Практическая работа № 49.

Развертывание рабочего места помощника главного администратора.

Цель работы: освоение приемов развертывания рабочего места помощника главного администратора.

Практическая работа № 50.
Миграция ПО ViPNet Administrator.
Цель работы: освоение приемов миграции ПО ViPNet Administrator.
Практическая работа № 51.
Модификация защищенной сети.
Цель работы: освоение приемов модификации защищенной сети.
Практическая работа № 52.
Смена пароля администратора УКЦ. Смена мастер-ключей. Формирование нового сертификата ключа проверки электронной подписи.
Цель работы: освоение приемов смены пароля, мастер-ключей, сертификата ключа электронной подписи.
Практическая работа № 53.
Компрометация ключей пользователя.
Цель работы: освоение приемов работы с ситуацией компрометации ключей пользователя.

Тема 2.4. Центр управления политиками безопасности ViPNet Policy Manager
1. Перечень вопросов для устного или письменного опроса по теме:
1. Принципы централизованного управления политиками безопасности сетевых узлов.
2. Основные возможности ViPNet Policy Manager.
3. Формирование результирующей политики безопасности.

2. Тематика практических работ:
Практическая работа № 54.
Настройка политик безопасности в ViPNet Policy Manager.
Цель работы: освоение приемов настройки политик безопасности в ViPNet Policy Manager.

Тема 2.5. Координатор
1. Перечень вопросов для устного или письменного опроса по теме:
1. Функциональные возможности Координатора.
2. Общие принципы взаимодействия сетевых узлов (СУ).
3. Сервер IP-адресов.
4. Сервер-Маршрутизатор.
5. Сервер-Межсетевой экран.
6. Режимы работы узлов VipNet.
7. Маршрутизация трафика.
8. Общие сведения.
9. Принципы формирования.
10. Протокол OSPF.
11. Статическая маршрутизация.
12. Балансировка IP-трафика.
13. Обработка прикладных протоколов.
14. Агрегация сетевых интерфейсов.
15. Туннелирование незащищенных узлов.
16. Фильтрация трафика.
17. Антиспуфинг.
18. Понятие технологии трансляции сетевых адресов NAT.
19. Реализация NAT в Координаторе.

20. Сервер открытого Интернета.

Тема 2.6. Программно-аппаратный комплекс (ПАК) Координатор VipNet HW4

1. Перечень вопросов для устного или письменного опроса по теме:

1. ПАК VipNet Coordinator HW4.
2. Назначение.
3. Функциональные возможности.
4. Общий обзор базовой линейки программно-аппаратных комплексов VipNet.
5. Администрирование.
6. Сценарии применения ПАК.
7. Программное обеспечение ПАК VipNet Coordinator HW.
8. Инсталляция ПО.
9. Верификация образа ПО.
10. Запись образа ПО на носитель.
11. Развертывание ключевых баз.
12. Работа с командной строкой.
13. Общие принципы работы с конфигурационными файлами.
14. Удаленное управление ПАК.
15. Работа с веб-интерфейсом.

2. Самостоятельная работа:

1. Система защиты от сбоев.
2. Режимы работы: одиночный режим, режим кластера.

3. Тематика практических работ:

Практическая работа № 55.

Межсетевое взаимодействие. Установка VipNet Coordinator в качестве межсетевого шлюза. Первоначальная настройка межсетевого взаимодействия.

Цель работы: освоение приемов межсетевого взаимодействия, установки VipNet Coordinator.

Практическая работа № 56.

Модификация межсетевого взаимодействия.

Цель работы: освоение приемов модификации межсетевого взаимодействия.

Практическая работа № 57.

Firewall. Фильтры по умолчанию.

Цель работы: освоение приемов работы с Firewall.

Практическая работа № 58.

Фильтрация незащищенного локального трафика.

Цель работы: освоение приемов фильтрации незащищенного локального трафика.

Практическая работа № 59.

Фильтрация незащищенного транзитного трафика.

Цель работы: освоение приемов фильтрации незащищенного транзитного трафика.

Практическая работа № 60.

Включение антиспуфинга.

Цель работы: освоение приемов включения антиспуфинга.

Практическая работа № 61.

Настройка трансляции сетевых адресов.

Цель работы: освоение приемов настройки трансляции сетевых адресов.

Практическая работа № 62.
Фильтрация защищенного трафика.
Цель работы: освоение приемов фильтрации защищенного трафика.
Практическая работа № 63.
Настройка Автономного режима.
Цель работы: освоение приемов настройки автономного режима.
Практическая работа № 64.
Настройка полутуннеля.
Цель работы: освоение приемов настройки полутуннеля.
Практическая работа № 65.
Сохранение настроек ПАК.
Цель работы: освоение приемов сохранения настроек ПАК.
Практическая работа № 66.
Настройка расписания в правилах фильтрации.
Цель работы: освоение приемов настройки расписания в правилах фильтрации.
Практическая работа № 67.
Агрегация каналов.
Цель работы: освоение приемов агрегации каналов.
Практическая работа № 68.
Включение и настройка протокола динамической маршрутизации OSPF.
Цель работы: освоение приемов настройки протокола динамической маршрутизации OSPF.
Практическая работа № 69.
Настройка кластера горячего резервирования.
Цель работы: освоение приемов настройки кластера горячего резервирования.
Практическая работа № 70.
Криптопровайдер VipNet CSP. Работа с сертификатами. Работа с ЭП.
Цель работы: освоение приемов работы с криптопровайдером, сертификатами, электронной подписью.
Практическая работа № 71.
Работа с приложениями VipNet. Установка прямого взаимодействия по каналу MFTP.
Цель работы: освоение приемов работы с приложениями VipNet.
Практическая работа № 72.
Настройка автопроцессинга в программе ViPNet Деловая почта.
Цель работы: освоение приемов работы с Деловой почтой.
Практическая работа № 73.
Настройка взаимодействия сетей ViPNet.
Цель работы: освоение приемов настройки взаимодействия VipNet.
Практическая работа № 74.
Настройка межсетевого взаимодействия после компрометации ключевой информации.
Цель работы: освоение приемов настройки межсетевого взаимодействия после компрометации ключевой информации.

3.7. Типовые задания для промежуточного контроля по МДК.03.03 Корпоративная защита от внутренних угроз информационной безопасности

Вопросы к экзамену:

Конфигурация сетевой инфраструктуры: настройка хостмашины, сетевого окружения, виртуальных машин, и т.п.
2. Установка и настройка системы корпоративной защиты от внутренних угроз. Самостоятельный поиск и устранение неисправностей при развёртывании и настройке.
3. Установка и настройка агентского мониторинга.
4. Проведение синхронизации с LDAP -сервером, разделе персоны.
5. Запуск системы корпоративной защиты от внутренних угроз.
6. Угрозы информационной безопасности.
7. Изучение структуры организации на основании полученных материалов («модели организации»), проведение обследования корпоративных информационных систем. Определение объекта защиты.
8. Перечень субъектов/персон, сформулированных верно, роли пользователей, права доступа.
9. Политика безопасности.
10. Разработка новой и/или модифицирование существующей политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания.
11. Использование различных технологий защиты: печатей, бланков, графических объектов, баз данных и т.п.
12. Модифицирование политики безопасности в системе IWTM в соответствие с получаемыми на практике данными перехвата.
13. Применение политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором угроз. Максимизировать число выявленных инцидентов безопасности.
14. Работа с интерфейсом управления системы корпоративной защиты информации.
15. Технология анализа и защиты сетевого трафика.
16. Развёртывание, настройка и проверка работоспособности VPN -сети на существующей и вычислительной инфраструктуре.
17. Развёртывание, настройка и проверка работоспособности IDS -системы на существующей и вычислительной.
18. Работа с узлами и пользователями. VPN. Компрометация узлов, ключей, пользователей. Восстановление связи.
19. Обновление ключевой информации. VPN. Межсетевое взаимодействие и туннелированные. VPN.
20. Централизованная политика безопасности.
21. Защита рабочих мест. IDS. Выявление большей части инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий.
22. Технологии агентского мониторинга.
23. Демонстрация знания механизмов работы агентского мониторинга.
24. Разработать и применить политику агентского мониторинга для работы с носителями и устройствами.
25. Разработка и применение политики агентского мониторинга для работы с файлами. Работа с исключениями из перехвата.
26. Анализ выявленных инцидентов. Подготовка отчётов о нарушениях.
27. Применение механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов.
28. Проведение классификацию уровня угроз инцидентов.

29. Оценка ущерба. Использование дополнительных модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса.
30. Выявление инцидентов и противодействие нарушителям с опорой на нормативную базу.

3.8. Требования к дифференцированному зачету по учебной практике

Контроль и оценка результатов освоения учебной практики осуществляются руководителем практики в процессе проведения учебных занятий, самостоятельного выполнения обучающимися заданий, выполнения практических проверочных работ. В результате освоения учебной практики в рамках профессиональных модулей обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета.

Приобретенные навыки обучающегося кладутся в основу определения качества полученных знаний по учебной практике и являются основными критериями их оценки на зачете:

- правильно эксплуатирует системы и средства, предназначенные для эффективного функционирования комплексной системы защиты информации в подразделениях организации;
- использует методы и средства защиты данных;
- планирует организационные мероприятия, проводимые при криптографической защите информации;
- устанавливает и настраивает средства защиты информации;
- администрирует системы защиты информации;
- создает и модифицирует защищенные сети по заданным схемам;
- организовывает межсетевое взаимодействие;
- организовывает взаимодействия всех объектов VPN между собой и функционирования туннеля;
- обеспечивает работу сервера защищенных соединений;
- применяет общие положения об информационной безопасности для телекоммуникационных систем;
- использует организационно-технические и правовые основы использования электронного документооборота в информационных системах;
- создает структуру виртуальной защищенной сети;
- применяет технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений;
- использует основные компоненты системы защиты информации, состав программного комплекса ViPNet (Administrator, Client, Coordinator);
- применяет основные функции и возможности комплекса ViPNet, прикладные системы комплекса ViPNet;
- работает с ключевой структурой сети ViPNet (ключевая система, формирование и управление ключевой системой);
- применяет знания ЦУС и УКЦ: функции и условия их взаимодействия.

Критерии оценки защиты отчета по учебной практике:

– Оценка «отлично» выставляется обучающемуся, если он глубоко и прочно усвоил программный материал дисциплины, исчерпывающе, последовательно, четко и логически

стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами и вопросами, не затрудняется с ответами при видоизменении заданий, правильно обосновывает принятые решения, владеет разносторонними навыками и приемами выполнения практических задач;

– Оценка «хорошо» выставляется обучающемуся, если он твердо знает материал курса, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения;

– Оценка «удовлетворительно» выставляется обучающемуся, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических задач;

– Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно.

3.9. Требования к дифференцированному зачету по производственной практике

Дифференцированный зачет по производственной практике выставляется с учетом данных Дневника отчета по практике с указанием: видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика; отчетом по производственной практике; аттестационного листа практиканта; оценки освоения общих компетенций по результатам практики; характеристики профессиональной деятельности обучающегося на практике.

Оценочные материалы

Перечень вопросов к собеседованию по производственной практике:

1. Краткая характеристика места практики.
2. Выявление и оценка рисков, связанных с внутренними угрозами информационной безопасности предприятия;
3. Выявление каналов передачи информации, подлежащие защите средствами автоматизированных систем контроля информационных потоков организации;
4. Проведение аудита информационных активов предприятия и бизнес-контекст их обработки в ИС предприятия в соответствии с принятыми процессами и процедурами;
5. Разработка и внедрение политики внутренней информационной безопасности;
6. Применение нормативно-правовой основы для внедрения и использования систем автоматизированного контроля информационных потоков класса DLP и проведения служебных расследований инцидентов внутренней информационной безопасности;
7. Администрирование и использование в профессиональной деятельности системы контроля информационных потоков организации, проведение расследования инцидентов информационной безопасности и подготовка соответствующих отчетов.

4. Контрольно-оценочные средства для проведения экзамена по профессиональному модулю

4.1 Паспорт

Экзамен по профессиональному модулю предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.03 Защита информации техническими средствами.

Условием допуска к квалификационному экзамену являются положительные аттестации: по промежуточной аттестации МДК.03.01, МДК.03.02, МДК.03.03, по учебной практике УП.03, по производственной практике ПП.03.

Результаты освоения модуля, подлежащие проверке на квалификационном экзамене, являются общие и профессиональные компетенции ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10, ПК 3.1. ПК. 3.2. ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6, ПК 3.7, ПК 3.8, ПК 3.9 .

4.2 Задания для экзаменующегося

Инструкция: Внимательно прочитайте задание. Вы можете воспользоваться персональным компьютером, необходимыми периферийными устройствами, справочной литературой, программным обеспечением, ресурсами глобальной сети Интернет.
Время выполнения задания – 30 минут.

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы).

Задание 1

Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.
Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину нарушителя для удаленного доступа к серверу агентского мониторинга.
Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.
Имя пользователя: user1, пароль: 12345678
Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании. Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.
Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах. Зафиксировать создание политики скриншотом.

Задание 8

Необходимо поставить на контроль печать документов на принтерах. Продемонстрировать работоспособность на любую из политик.
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.
Проверить работоспособность и зафиксировать выполнение: продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 10

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.
Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 12

Создайте локальную группу пользователей «Сотрудники под наблюдением».
Добавьте в нее трех любых пользователей.
Подтвердите выполнение задания скриншотами.

Задание 13

Для работы системы необходимо настроить периметр компании: Почтовый домен: demo.lab. Список веб ресурсов необходимо создать и назвать «Доверенные домены»: filialdemo.lab, demolab-info.ru, dlpsystems.lab.
Группа персон 1: пользователи домена.
Исключить из перехвата почту генерального директора.
Подтвердите выполнение задания скриншотами.

Задание 14

Для недавно нанятого аудитора компании необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования.
Области видимости: все.
Логин: auditor, пароль: 12345678
Подтвердите выполнение задания скриншотами.

Политика 1

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с

этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills». Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например: «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).
Вердикт: разрешить √
Уровень нарушения: средний •
Тег: мобильники
Проверить работоспособность.

Политика 2

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.
Для пустого документа:
Вердикт: разрешить √
Уровень нарушения: нет
Тег: договор
Для заполненного документа:
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: договор
Проверить работоспособность.

Политика 3

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.
Вердикт: запретить ×
Уровень нарушения: средний •
Тег: бланк
Проверить работоспособность.

Политика 4

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: печать
Проверить работоспособность.

Политика 5

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (10 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.
Передача кодов внутри компании:
Вердикт: разрешить √

Уровень нарушения: низкий •
Тег: коды
Передача кодов за пределы компании:
Вердикт: запретить ×
Уровень нарушения: средний •
Тег: бланк
Проверить работоспособность.

Политика 6

Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации.
Вердикт: разрешить √
Уровень нарушения: средний •
Тег: база
Проверить работоспособность.

Политика 7

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: вирус
Проверить работоспособность.

Политика 8

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.
Вердикт: запретить ×
Уровень нарушения: высокий •
Тег: ПДн
Проверить работоспособность.

Задание 15: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:
Динамика активности по событиям за последнюю неделю
Статистика по политикам за последние 7 дней
По типу событий: необработанные нарушения за три дня
По топ-нарушителям за текущий месяц.

Задание 16: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:
Отображающий события с уровнем угрозы от низкого до высокого на

Задание 17

Создайте локальную группу пользователей «Сотрудники под наблюдением».
Добавьте в нее трех любых пользователей.
Подтвердите выполнение задания скриншотами.

Задание 18

Для работы системы необходимо настроить периметр компании: Почтовый домен: demo.lab. Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 19

Для недавно нанятого аудитора компании необходимо создать пользователя системы IWTM с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования.

Области видимости: все.

Логин: auditor, пароль: 12345678

Подтвердите выполнение задания скриншотами.

Политика 9

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills». Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например, «Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мобильники

Проверить работоспособность.

Политика 10

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Тег: договор

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 11.

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк
Проверить работоспособность.

Политика 12

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: печать
Проверить работоспособность.

Политика 13

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (8 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.
Передача кодов внутри компании:
Вердикт: разрешить √
Уровень нарушения: низкий •
Тег: коды
Передача кодов за пределы компании:
Вердикт: запретить ×
Уровень нарушения: средний •
Тег: бланк
Проверить работоспособность.

Политика 14

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания, планируется к внедрению в эксплуатацию. Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф. Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенно-цифирными кодами на русском языке:
Р-Цифры-Буквы или РЦифрыБуквы или Р-ЦифрыБуквы Р – русская буква «Р»
Цифры – не более 3-х подряд, например, 27 или 500 (обязательно наличие хотя бы одной цифры)
Буквы – от 2 до 3-х подряд, например, Р-27АЭ
Вердикт: запретить ×
Уровень нарушения: высокий •
Тег: ракеты
Проверить работоспособность.

Политика 15

Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации.
Вердикт: разрешить √
Уровень нарушения: средний •
Тег: база
Проверить работоспособность.

Политика 16

В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: подработка

Проверить работоспособность.

Политика 17

Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» любым сотрудникам за пределы компании. Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции, а также писать название компании на русском языке, например, «ООО Demo Лаб», «ООО Демо Лаб».

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: печать

Проверить работоспособность.

Политика 18

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу. Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 19

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: ПДн

Проверить работоспособность.

Политика 20

Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Задание 21: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю
Статистика по политикам за последние 7 дней
По типу событий: необработанные нарушения за три дня
По топ-нарушителям за текущий месяц.

Задание 22: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:
Отображающий события с уровнем угрозы от низкого до высокого на правила буфера обмена за последние 7 дней.
Отображающий события с любым одним тегом правила копирования (внешние носители, печать) за последние 7 дней.

4.3 Пакет экзаменатора

4.3.1. Условия выполнения задания:

Время выполнения каждого задания 40 минут. Обучающиеся могут воспользоваться ПК и необходимым программным обеспечением для выполнения задания.

Условием допуска студентов к экзамену наличие положительных оценок за элементы модуля: МДК.03.01, МДК.03.02, МДК.03.03 и учебной и производственной практик.

В результате аттестации по профессиональному модулю комплексная проверка профессиональных и общих компетенций профессионального модуля осуществляется в форме оценки качества выполнения практических заданий на квалификационном экзамене. Задания №1- №22, политики № 1-№19. выполняются в компьютерном классе.

4.3.2. Инструкция для экзаменатора

Ознакомьтесь с заданиями для экзаменующихся.
Время выполнения каждого задания на компьютере 40 минут.

4.3.3. Требования к процедуре оценки

Помещение: особых требований нет,
Оборудование: компьютер
Инструменты: особых требований нет
Расходные материалы: бумага для записей, оценочные ведомости
Доступ к дополнительным инструкциям и справочным материалам: не предусмотрен
Норма времени на выполнение практических заданий для студента: 40 минут.

4.4 Критерии оценки

Предметом оценки освоения дисциплины являются знания, умения, общие и профессиональные компетенции и способность применять их в практической, профессиональной деятельности.

Критерии оценок:

– оценка «отлично» ставится, за правильно выполненные задания; грамотно проведенный анализ программных продуктов, сделаны выводы; даны развернутые ответы на поставленные вопросы.

– оценка «хорошо» ставится, за правильно выполненные задания, но с небольшими недочетами; грамотно проведенный анализ программных продуктов, сделаны выводы; даны развернутые ответы на поставленные вопросы.

– оценка «удовлетворительно» ставится, за выполненное задание, но не в полном объеме; допущены несущественные ошибки при проведении анализа программных продуктов, сделаны выводы; даны ответы на поставленные вопросы в сжатом виде, знания показаны слабо, речь неграмотная.

– оценка «неудовлетворительно» ставится, за невыполненное задание; допущены грубейшие ошибки при проведении анализа программных продуктов, логика и последовательность изложения имеют существенные нарушения; ответы на поставленные вопросы отсутствуют, речь неграмотная.