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.02 Защита информации в автоматизированных системах программными и программно-аппаратными 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.02 Защита информации в автоматизированных системах программными и программно-аппаратными 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:

Глухова С.В.	Преподаватель компьютерных дисциплин ГБПОУ КК ПСХК, высшая квалификационная категория, физик, преподаватель, преподавание информатики в общеобразовательных учреждениях

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

СОДЕРЖАНИЕ

1. Паспорт комплекта контрольно-оценочных средств.

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения основной образовательной программы в целом.

Формой аттестации по профессиональному модулю является экзамен. Экзамен 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.02.01. Программные и программно-аппаратные средства защиты информации	Дифференцированный зачет	Контрольная работа	Устные ответы; Тестирование; Самостоятельные работы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Защита курсовой работы (курсового проекта)
МДК.02.02. Криптографические средства защиты информации	Экзамен	Контрольная работа	Устные ответы; Тестирование; Самостоятельные работы; Формализованное наблюдение и оценка выполнения и защиты практической работы;
УП.02	Дифференцированный зачет	-	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП.02	Дифференцированный зачет	-	Оценка выполнения работ и оформления отчетной документации на производственной практике

Профессиональный модуль ПМ.02	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
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	устанавливает программные и программно-аппаратные средства защиты информации; настраивает программные и программно-аппаратные средства защиты информации; применяет программные и программно-аппаратные средства защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных.
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно- аппаратными средствами.	устанавливает средства антивирусной защиты; настраивает средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливает программные и программно- аппаратные средства защиты информации; настраивает программные и программно- аппаратные средства защиты информации; применяет системы контроля и управления доступом для защиты информации; проверяет выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	проводит диагностику программно-аппаратных средств защиты информации; устраняет отказы в работе программно-аппаратных средств защиты информации; обеспечивает работоспособность программно- аппаратных средств защиты информации; тестирует функции программно-аппаратных средств защиты информации; восстанавливает работоспособность программных и программно-аппаратных средств защиты информации**.**
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	применяет симметричные и асимметричные криптографические алгоритмы и средства шифрования данных; применяет программные и программно- аппаратные средства для защиты информации в базах данных; проверяет выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по

	требованиям безопасности информации; применяет математический аппарат для выполнения криптографических преобразований; использует типовые программные криптографические средства, в том числе электронную подпись
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	ведет учёт информации, для которой установлен режим конфиденциальности; обрабатывает информацию, для которой установлен режим конфиденциальности; обеспечивает надежное хранение информации, для которой установлен режим конфиденциальности; передает информацию, для которой установлен режим конфиденциальности, с соблюдением установленных требований; применяет средства гарантированного уничтожения информации
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	работает с подсистемами регистрации событий; выявляет события и инциденты безопасности в автоматизированной системе; устанавливает программные и программно-аппаратные средства защиты информации; настраивает программные и программно-аппаратные средства защиты информации; применяет программные и программно-аппаратные средства защиты информации; осуществляет мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	распознает задачу и/или проблему в профессиональном контексте; анализирует задачу и/или проблему и выделяет её составные части; определяет этапы решения задачи; выявляет и осуществляет поиск информации, необходимой 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, выделяет в нём сильные и слабые стороны
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 в

	соответствии с параметрами поиска; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; интерпретирует полученную информацию в контексте профессиональной деятельности; оформляет результаты поиска
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	использует актуальную нормативно-правовую документацию по специальности; применяет современную научно профессиональную терминологию; определяет актуальность нормативно-правовой документации в профессиональной деятельности; выстраивает траектории профессионального и личностного развития; участвует в конкурсах профессионального мастерства; участвует в мероприятиях профессиональной направленности (вебинары, семинары, конференции, круглые столы, форумы и т.д.)
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	участвует в деловом общении для эффективного решения деловых задач; планирует профессиональную деятельность; организует работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами; при групповом обсуждении задает вопросы для понимания идей других; при групповом обсуждении: убеждается, что коллеги по группе поняли предложенную идею; участвует в деятельности по выявлению ресурсов команды; анализирует работу членов группы; анализирует результаты выполненного задания; презентует результаты работы группы; защищает полученные командой результаты
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	грамотно (устно и письменно) излагает свои мысли по профессиональной тематике на государственном языке; проявляет толерантность в рабочем коллективе; извлекает из устной речи (монолог, диалог, дискуссия) нужную информацию и логические связи, организующие эту информацию; грамотно оформляет документы на государственном языке; корректно общается с преподавателями и одногруппниками; соблюдает заданный жанр высказывания (служебный доклад, выступление на совещании / собрании, презентация товара / услуг); корректно отвечает на вопросы, направленные на выяснение мнения (позиции); задает четко

	сформулированные вопросы, направленные на получение необходимой информации.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	соблюдает нормы поведения во время учебных занятий и прохождения учебной и производственной практик; понимать значимость своей специальности; демонстрирует поведение на основе общечеловеческих ценностей
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	эффективность выполнения правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик; использует ресурсосберегающие технологии в профессиональной деятельности, на рабочем месте.
ОК 09. Использовать информационные технологии в профессиональной деятельности	ориентируется в информационно-коммуникационных технологиях, применяемых в профессиональной деятельности; применяет средства информатизации и информационных технологий для реализации профессиональной деятельности; в профессиональной деятельности использует современное программное обеспечение; представляет информацию в различных формах с использованием разнообразного программного обеспечения; способен адаптироваться в новых программных продуктах
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые); понимает тексты на базовые профессиональные темы; применяет в профессиональной деятельности инструкции на государственном и иностранном языке; строит простые высказывания о себе и о своей профессиональной деятельности; пишет простые связные сообщения на знакомые или интересующие профессиональные темы.

3. Оценка освоения профессионального модуля:

3.1. Типовые задания для текущего контроля по МДК.02.01. Программные и программно- аппаратные средства защиты информации

Тема 1.1 Предмет и задачи программно-аппаратной защиты информации.

Вопросы для устного опроса

1. Предмет и задачи программно-аппаратной защиты информации.
2. Основные понятия программно-аппаратной защиты информации.
3. Классификация методов и средств программно-аппаратной защиты информации

Тема 1.2 Стандарты безопасности.

Вопросы для устного опроса

1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно- аппаратными средствами.
2. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).
3. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Практическая работа № 1

Тема: Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.

Практическая работа № 2

Тема: Применение нормативных документов по противодействию технической разведке

Практическая работа № 3

Тема: Обзор стандартов. Работа с содержанием стандартов

Практическая работа № 4

Тема: Применение нормативных документов для оценки уязвимости

Тема 1.3 Защищенная автоматизированная система.

Вопросы для устного опроса

1. Автоматизация процесса обработки информации.
2. Понятие автоматизированной системы.
3. Особенности автоматизированных систем в защищенном исполнении.
4. Основные виды АС в защищенном исполнении.
5. Методы создания безопасных систем.
6. Методология проектирования гарантированно защищенных КС.
7. Дискреционные модели.
8. Мандатные модели.

Практическая работа № 5

Тема: Учет, обработка, хранение и передача информации в АИС

Практическая работа № 6

Тема: Определение параметров настройки программного обеспечения и системы защиты информации автоматизированной системы

Практическая работа № 7

Тема: Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа. Регистрация событий (аудит).

Практическая работа № 8

Тема: Реализация правил разграничения доступа персонала к объектам доступа

Практическая работа № 9

Тема: Контроль целостности данных. Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности.

Практическая работа № 10
Тема: Настройка параметров программного обеспечения системы защиты информации автоматизированной системы.
Практическая работа № 11
Тема: Криптографическая защита. Обзор программ шифрования данных.

Тема 1.4 Дестабилизирующее воздействие на объекты защиты.
Вопросы для устного опроса
1. Источники дестабилизирующего воздействия на объекты защиты.
2. Способы воздействия на информацию.
3. Причины и условия дестабилизирующего воздействия на информацию.

Практическая работа № 12
Тема: Определение причин и условий дестабилизирующего воздействия на информацию
Практическая работа № 13
Тема: Методика выявления способов воздействия на информацию
Практическая работа № 14
Тема: Распределение каналов в соответствии с источниками воздействия на информацию
Практическая работа № 15
Тема: Классификация каналов утечки информации

Тема 1.5 Принципы программно-аппаратной защиты информации от несанкционированного доступа.
Вопросы для устного опроса
1. Понятие несанкционированного доступа к информации.
2. Основные подходы к защите информации от НСД.
3. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
4. Доступ к данным со стороны процесса.
5. Особенности защиты данных от изменения. Шифрование.

Практическая работа № 16
Тема: Организация доступа к файлам
Практическая работа № 17
Тема: Защита носителей информации
Практическая работа № 18
Тема: Выбор надежного оборудования
Практическая работа № 19
Тема: Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД
Практическая работа № 20
Тема: Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД

Тема 2.1 Основы защиты автономных автоматизированных систем.
Вопросы для устного опроса
1. Работа с автономной АС в защищенном режиме.
2. Алгоритм загрузки ОС. Штатные средства замыкания среды.

3. Расширение BIOS как средство замыкания программной среды.
4. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды.
1. Понятие АМДЗ (доверенная загрузка).
5. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.

Практическая работа № 21

Тема: Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. ГОСТ Р 51583-2014 Защита информации.

Практическая работа № 22

Тема: Особенности построения защищенных автоматизированных систем на основе существующих компонентов

Практическая работа № 23

Тема: Уровни контроля на отсутствие недекларированных возможностей (НДВ) в ПО средств защиты информации

Тема 2.2 Защита программ от изучения.

Вопросы для устного опроса

1. Изучение и обратное проектирование ПО.
2. Способы изучения ПО: статическое и динамическое изучение.
3. Задачи защиты от изучения и способы их решения.
4. Защита от отладки.
5. Защита от дизассемблирования.
6. Защита от трассировки по прерываниям

Тема 2.3 Вредоносное программное обеспечение.

Вопросы для устного опроса

1. Вредоносное программное обеспечение как особый вид разрушающих воздействий.
2. Классификация вредоносного программного обеспечения.
3. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
4. Поиск следов активности вредоносного ПО.
5. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО.
6. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.
7. Ботнеты. Принцип функционирования. Методы обнаружения.
8. Классификация антивирусных средств. Сигнатурный и эвристический анализ.
9. Защита от вирусов в "ручном режиме".
10. Основные концепции построения систем антивирусной защиты на предприятии.

Практическая работа № 24

Тема: Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО

Практическая работа № 25

Тема: Ответственность за создание, использование и распространение вредоносного ПО.

Практическая работа № 26

Тема: Построение системы антивирусной защиты серверов и рабочих станций

Практическая работа № 27

Тема: Системы обнаружения и предотвращения вторжений (IDS, IPS).

Практическая работа № 28
Тема: Разработка стратегического плана построения системы защиты
Практическая работа № 29
Тема: Разработка методов реагирования в случае инцидентов и восстановление

Тема 2.4 Защита программ и данных от несанкционированного копирования.
Вопросы для устного опроса

1. Несанкционированное копирование программ как тип НСД.
2. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.
3. Привязка ПО к аппаратному окружению и носителям.
4. Защитные механизмы в современном программном обеспечении на примере MS Office.

Практическая работа № 30
Тема: Защита информации от несанкционированного копирования с использованием специализированных программных средств
Практическая работа № 31
Тема: Защитные механизмы в приложениях (на примере MSWord, MS Excel, MS PowerPoint)
Практическая работа № 32
Тема: Реализация защитных механизмов в приложениях свободно-распространяемого ПО.

Тема 2.5 Защита информации на машинных носителях.
Вопросы для устного опроса

1. Проблема защиты отчуждаемых компонентов ПЭВМ.
2. Методы защиты информации на отчуждаемых носителях. Шифрование.
3. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
4. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.
5. Безвозвратное удаление данных. Принципы и алгоритмы.

Практическая работа № 33
Тема: Применение средства восстановления остаточной информации на примере Foremost или аналога
Практическая работа № 34
Тема: Применение специализированного программного средства для восстановления удаленных файлов. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*
Практическая работа № 35
Тема: Применение программ для безвозвратного удаления данных
Практическая работа № 36
Тема: Применение программ для шифрования данных на съемных носителях. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации.*

Тема 2.6 Аппаратные средства идентификации и аутентификации пользователей.

Вопросы для устного опроса

1. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ.
2. Устройства Touch Memory.

Тема 2.7 Системы обнаружения атак и вторжений.

Вопросы для устного опроса

1. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.
2. Использование сетевых снифферов в качестве СОВ.
3. Аппаратный компонент СОВ.
4. Программный компонент СОВ.
5. Модели системы обнаружения вторжений.
6. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий.
7. Другие методы обнаружения вторжений.

Практическая работа № 37

Тема: Моделирование проведения атаки

Практическая работа № 38

Тема: Изучение инструментальных средств обнаружения вторжений. *Устранение известных уязвимостей автоматизированной системы, приводящих к возникновению угроз безопасности информации*

Практическая работа № 39

Тема: *Анализ методов обнаружения злоупотреблений. Методы, основанные на моделировании поведения злоумышленника*

Тема 3.1 Основы построения защищенных сетей.

Вопросы для устного опроса

1. Сети, работающие по технологии коммутации пакетов.
2. Стек протоколов TCP/IP. Особенности маршрутизации.
3. Штатные средства защиты информации стека протоколов TCP/IP.
4. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

Практическая работа № 40

Тема: *Подготовка и технологии проведения и создания карты покрытия*

Практическая работа № 41

Тема: *Реализация технологий брандмауэра*

Практическая работа № 42

Тема: *Линейка оборудования для беспроводных сетей.*

Тема 3.2 Средства организации VPN.

Вопросы для устного опроса

1. Виртуальная частная сеть. Функции, назначение, принцип построения.
2. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
3. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.
4. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.

Практическая работа № 43
Тема: Развертывание VPN.
Практическая работа № 44
Тема: Развертывание VPN.
Практическая работа № 45
Тема: *Разработка предложений по совершенствованию системы управления защиты информации автоматизированной системы.*

Тема 4.1 Обеспечение безопасности межсетевого взаимодействия.
Вопросы для устного опроса

1. Методы защиты информации при работе в сетях общего доступа.
2. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.
3. Основные типы firewall. Симметричные и несимметричные firewall.
4. Уровень 1. Пакетные фильтры.
5. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.
6. Уровень 3. Proxy-сервера прикладного уровня.
7. Однохостовые и мультихостовые firewall.
8. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.
9. Требования по сертификации межсетевых экранов.

Практическая работа № 46
Тема: Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimeter. *Управление рисками*
Практическая работа № 47
Тема: Изучение различных способов закрытия "опасных" портов. *Применение механизмов и служб защиты*

Тема 5.1 Защита информации в базах данных.
Вопросы для устного опроса

1. Основные типы угроз. Модель нарушителя.
2. Средства идентификации и аутентификации. Управление доступом.
3. Средства контроля целостности информации в базах данных.
4. Средства аудита и контроля безопасности. Критерии защищенности баз данных.
5. Применение криптографических средств защиты информации в базах данных.

Практическая работа № 48
Тема: Изучение механизмов защиты СУБД MS Access. *Правила безопасности и доступа*
Практическая работа № 49
Тема: Изучение штатных средств защиты СУБД MSSQL Server. *Протокол SSL*
Практическая работа № 50
Тема: Средства создания резервных копий и восстановления баз данных

Тема 6.1 Мониторинг систем защиты.
Вопросы для устного опроса

1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.
2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25.
3. Классификация отслеживаемых событий. Особенности построения систем мониторинга.
4. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.
5. Классификация сетевых мониторов.
6. Системы управления событиями информационной безопасности (SIEM).
7. Обзор SIEM-систем на мировом и российском рынке.

Практическая работа № 51

Тема: Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов

Практическая работа № 52

Тема: *Анализ программных, архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей систем защиты информации автоматизированных систем*

Практическая работа № 53

Тема: Проведение аудита ЛВС сетевым сканером

Практическая работа № 54

Тема: *Определение методов управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе*

Тема 6.2 Изучение мер защиты информации в информационных системах.

Вопросы для устного опроса

1. Требования к защите информации, не составляющей государственную тайну.
2. Методические документы ФСТЭК по применению мер защиты.

Практическая работа № 55

Тема: Выбор мер защиты информации для их реализации в информационной системе. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*

Практическая работа № 56

Тема: Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке. *Применение аналитических и компьютерных моделей автоматизированных систем и систем защиты информации*

Тема 6.3 Изучение современных программно-аппаратных комплексов

Практическая работа № 57

Тема: Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. *Обеспечение безопасности рабочих станций и серверов*

Практическая работа № 58

Тема: Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*

Практическая работа № 59

Тема: Изучение типовых решений для построения VPN на примере VIP Net или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*

Практическая работа № 60

Тема: Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. *Обеспечение безопасности рабочих станций и серверов*

Практическая работа № 61

Тема: Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов. *Обеспечение безопасности рабочих станций и серверов.*

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.

2. Тест

1)Информационная безопасность – это состояние

1. Конфиденциальности, непрерывности, доступности
2. Доступности, целостности, конфиденциальности
3. Непрерывности, доступности, целостности
4. Целостности, надежности, конфиденциальности.

2) Техническое, программное средство, вещество и материал, предназначенные или используемые для защиты информации

1. Система защиты информации автоматизированной системы
2. Система защиты информации
3. Средство защиты информации

3) Процедура проверки подлинности

1. Идентификация

2. Аутентификация

3. Авторизация

4) Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

1. Автоматическая система

2. Автоматизированная система

3. Информационная система

4. Система контроля и управления доступом

5) Объектом защиты информации могут являться

1. Компьютер, компьютерные сети, базы данных

2. Информационные системы, психологическое состояние пользователей

3. Бизнес-ориентированные, коммерческие системы

6) Источник дестабилизирующего воздействия на информацию

1. Бумажные носители информации

2. USB -устройства

3. Трудовой договор работника

7) К внешнему нарушителю относятся

1. Студенты, проходящие практику

2. Поставщики оборудования

3. Руководители

4. Отдел кадров

8) НСД – это

1. Доступ к информации, осуществляемый с нарушением установленных прав и правил доступа.

2. Разрушение или повреждение помещения для противозаконного проникновения в них или выхода из них.

3. Возможность проникновения в соответствии с установленными правилами и нормами.

4. Состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

9) Гипервизор - это

1. Это механизм создания виртуального представления ресурсов без привязки к аппаратному обеспечению.

2. Технология развертывания программного обеспечения на физическом оборудовании с использованием виртуализации.

3. Выделенный или специализированный компьютер для выполнения сервисного программного обеспечения

10) Что является из перечисленного вредоносным ПО

1. Backdoors, Руткит

2. Руткит, daemon tl

3. Загрузчик, Metasploit

4. Троян, Nmap

11) Сколько существует классов АС

1. 8

2. 9

3. 10

4. 11

12) Приведите примеры программных, аппаратных и программно-аппаратных средств защиты информации

13) Напишите, как происходит процесс аутентификации, идентификации, авторизации

14) Напишите основные документы в области защиты информации

15) Напишите основные модели безопасности информации и отличия между ними

16) Опишите на выбор 3 любых вредоносных ПО (что из себя представляет, чем опасен) и как от них защититься

3.2. Типовые задания для рубежного контроля по МДК.02.01. Программные и программно- аппаратные средства защиты информации

Контрольная работа № 1 «Защита информационных систем».

Задание. Ответить письменно на поставленные вопросы

Вариант 1

Ответьте письменно на поставленные вопросы:

1. Классификация методов и средств программно-аппаратной защиты информации.
2. Источники дестабилизирующего воздействия на объекты защиты.
3. Основные подходы к защите информации от НСД.
4. Работа автономной АС в защищенном режиме.
5. Методы защиты информации на отчуждаемых носителях. Шифрование.

Вариант 2

Ответьте письменно на поставленные вопросы:

1. Основные виды АС в защищенном исполнении.
2. Причины и условия дестабилизирующего воздействия на информацию.
3. Особенности защиты данных от изменения. Шифрование.
4. Вредоносное программное обеспечение как особый вид разрушающих воздействий.
5. Несанкционированное копирование программ как тип НСД.

Критерии оценок:

Оценкой «отлично» оцениваются ответы, которые показывают прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, давать аргументированные ответы, приводить примеры.

Оценкой «хорошо» оцениваются ответы, обнаруживающие прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, приводить примеры. Однако допускаются две-три неточности в ответах.

Оценкой «удовлетворительно» оцениваются ответы, свидетельствующие в основном о знании материалов, их свойств, технологий, но отличающиеся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа тем изучаемой дисциплины, недостаточным умением давать

аргументированные ответы и приводить примеры. Допускается несколько ошибок в содержании ответа.

Оценкой «неудовлетворительно» оцениваются ответы, обнаруживающие незнание материалов, их свойств, технологий изучаемой предметной области, отличающиеся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа тем изучаемой дисциплины; неумением давать аргументированные ответы. Допускаются серьезные ошибки в содержании ответов.

3.3. Типовые задания для промежуточного контроля по МДК.02.01. Программные и программно- аппаратные средства защиты информации

Вопросы к дифференцированному зачету

1. Предмет и задачи программно-аппаратной защиты информации.
2. Классификация методов и средств программно-аппаратной защиты информации.
3. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно- аппаратными средствами.
4. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
5. Методы создания безопасных систем.
6. Методология проектирования гарантированно защищенных КС.
7. Источники дестабилизирующего воздействия на объекты защиты.
8. Причины и условия дестабилизирующего воздействия на информацию.
9. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД.
10. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
11. Особенности защиты данных от изменения. Шифрование.
12. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка).
13. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.
14. Задачи защиты ПО от изучения и способы их решения. Защита ПО от дизассемблирования.
15. Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения.
16. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
17. Поиск следов активности вредоносного ПО.
18. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО.
19. Ботнеты. Принцип функционирования. Методы обнаружения.
20. Классификация антивирусных средств. Сигнатурный и эвристический анализ.
21. Защита от вирусов в "ручном режиме".
22. Основные концепции построения систем антивирусной защиты на предприятии.
23. Несанкционированное копирование программ как тип НСД.

24. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.
25. Защитные механизмы в современном программном обеспечении на примере MS Office.
26. Проблема защиты отчуждаемых компонентов ПЭВМ.
27. Методы защиты информации на отчуждаемых носителях. Шифрование.
28. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
29. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.
30. Безвозвратное удаление данных. Принципы и алгоритмы.
31. Устройства Touch Memory.
32. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.
33. Использование сетевых снифферов в качестве СОВ.
34. Аппаратный компонент СОВ. Программный компонент СОВ.
35. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий.
36. Штатные средства защиты информации стека протоколов TCP/IP.
37. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.
38. Виртуальная частная сеть. Функции, назначение, принцип построения.
39. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.
40. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.
41. Основные типы firewall. Симметричные и несимметричные firewall.
42. Однохостовые и мультихостовые firewall.
43. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту, исходя из архитектуры и выполняемых функций.
44. Основные типы угроз. Модель нарушителя.
45. Средства идентификации и аутентификации. Управление доступом.
46. Средства контроля целостности информации в базах данных.
47. Средства аудита и контроля безопасности. Критерии защищенности баз данных.
48. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.
49. Классификация сетевых мониторов.
50. Системы управления событиями информационной безопасности (SIEM).

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.

3.4. Тематика курсовых работ по МДК.02.01. Программные и программно-аппаратные средства защиты информации

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

1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание).
2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)
4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)
5. Проблема защиты информации в облачных хранилищах данных и ЦОДах
6. Защита сред виртуализации.
7. Виброакустические средства современных систем обеспечения информационной безопасности.
8. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.
9. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
10. Средства обеспечения информационной безопасности банков данных.
11. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
12. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.
13. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.
14. Обеспечение защиты конфиденциальной информации в распределенных системах разграничения доступа.
15. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.
16. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.

17. Инструментальные средства анализа рисков информационной безопасности.
18. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
19. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).
20. Анализ методов и средств анализа защищенности беспроводных сетей.
21. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
22. Программно-аппаратные средства защиты информационных ресурсов от несанкционированного использования и копирования.
23. Варианты решения антивирусной защиты корпоративной сети.
24. Корпоративная защита от внутренних угроз на базе DLP-системы
25. Организация защиты информации техническими средствами на предприятии
26. Организация защиты информации в системах контроля и управления доступом.
27. Организация защиты компьютерной сети предприятия от внешних вторжений
28. Применение систем контроля и учета действий персонала на предприятии
29. Применение программных снифферов для анализа сетевого трафика
30. Организация защиты информации в современных центрах обработки данных

3.5. Типовые задания для текущего контроля по МДК.02.02. Криптографические средства защиты информации

Тема 1.1 Математические основы криптографии
Вопросы для устного опроса
Вопросы по сравнению:

1. Покажите различие между Z и Z_n. Какое из этих множеств может содержать отрицательные целые числа? Как мы можем отобразить целое число в Z в целое число в Z_n? 2. Перечислите четыре свойства теории делимости, обсужденной в лекции.
2. Приведите пример целого числа с единственным делителем. Приведите пример целого числа только с двумя делителями. Приведите пример целого числа с более чем двумя делителями.
3. Определите наибольший общий делитель двух целых чисел. Какой алгоритм может эффективно найти наибольший общий делитель?
4. Что такое линейное диофантово уравнение двух переменных? Сколько решений может иметь такое уравнение? Как может быть найдено решение(я)?
5. Что такое оператор по модулю и какие у него имеются приложения? Перечислите все свойства, которые мы упоминали в этой лекции для операций по модулю.
6. Определите сравнение и сопоставьте его свойства со свойствами равенства.
7. Определите систему вычетов и наименьший вычет.
8. Какова разница между множеством Z_n и множеством Z_n^*? В каком множестве каждый элемент имеет аддитивную инверсию? В каком множестве каждый элемент имеет мультипликативную инверсию? Какой алгоритм используется, чтобы найти мультипликативную инверсию целого числа в Z_n?
9. Дайте определение матрицы. Что такое матрица-строка? Что такое матрица- столбец? Что такое квадратная матрица? Какая матрица имеет детерминант? Какая матрица может иметь инверсию?

10. Определите линейное сравнение. Какой алгоритм может использоваться, чтобы решить уравнение? Как мы можем решить набор линейных уравнений?

Вопросы по полям:

1. Определите алгебраическую структуру и назовите три алгебраических структуры, обсужденные в этой лекции.
2. Определите группу и приведите различия между группой и коммутативной группой
3. Определите кольцо и приведите различия между кольцом и коммутативным кольцом.
4. Определите поле и приведите различия между бесконечным полем и конечным полем.
5. Покажите число элементов в поле Галуа для простого числа.
6. Дайте один пример группы, использующей множество вычетов (операций по модулю).
7. Дайте один пример кольца, использующего множество вычетов (операций по модулю).
8. Дайте один пример поля, использующего множество вычетов (операций по модулю).
9. Покажите, как полином может представить n-битовое слово.
10. Определите неприводимый полином.

Практическая работа № 1

Тема: Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений

Практическая работа № 2

Тема: *Алгоритм быстрого возведения в степень по модулю.*

Практическая работа № 3

Тема: Проверка чисел на простоту

Практическая работа № 4

Тема: Решение задач с элементами теории чисел

Практическая работа № 5

Тема: *Методы разложения чисел на множители.*

Практическая работа № 6

Тема: *Исследование арифметических операции над большими числами*

Практическая работа № 7

Тема: *Исследование эллиптических кривых и их приложения в криптографии.*

Тема 2.1 Методы криптографической защиты информации

Вопросы для устного опроса

1. Определите шифр с симметричным ключом.
2. Поясните отличия между шифром подстановки и шифром перестановки.
3. Поясните отличия между моноалфавитным и многоалфавитным шифрами.
4. Поясните отличия между шифром потока и блочным шифром.
5. Все ли шифры потока являются моноалфавитными? Поясните.
6. Все ли блочные шифры являются многоалфавитными? Поясните.
7. Перечислите три моноалфавитных шифра.
8. Перечислите три многоалфавитных шифра.
9. Перечислите два шифра перестановки.
10. Перечислите четыре вида атак криптоанализ

Практическая работа № 8

Тема: Применение классических шифров замены

Практическая работа № 9

Тема: *Исследование и составление алгоритма применения классических шифров замены*

Практическая работа № 10

Тема: Применение классических шифров перестановки

Практическая работа № 11

Тема: *Исследование и составление алгоритма применения классических шифров перестановки*

Практическая работа № 12

Тема: Применение метода гаммирования

Практическая работа № 13

Тема: *Исследование и составление алгоритма применения метода гаммирования*

Тема 2.2 Криптоанализ

Вопросы для устного опроса

1. Основные методы криптоанализа. Криптографические атаки.
2. Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Керкхоффса.
3. Перспективные направления криптоанализа, квантовый криптоанализ.

Практическая работа № 14

Тема: Криптоанализ шифра простой замены методом анализа частотности символов

Практическая работа № 15

Тема: Криптоанализ шифра простой замены методом анализа частотности символов

Практическая работа № 16

Тема: Криптоанализ классических шифров методом полного перебора ключей

Практическая работа № 17

Тема: Криптоанализ классических шифров методом полного перебора ключей

Практическая работа № 18

Тема: Криптоанализ шифра Вижинера

Тема 2.3 Поточные шифры и генераторы псевдослучайных чисел

Вопросы для устного опроса

1. Блок транспозиции имеет 10 входов и 10 выходов. Каков порядок группы перестановки? Каков размер ключевой последовательности?
2. Блок подстановки имеет 10 входов и 10 выходов. Каков порядок группы перестановки? Каков размер ключевой последовательности?
3. Чем поточный шифр отличается от блочного?
4. Каким образом организуется шифрование потока данных переменной длины?
5. Какие числа называют "псевдослучайными"?
6. Какими свойствами должен обладать генератор псевдослучайных чисел для использования в криптографических целях?
7. Какие генераторы псевдослучайных чисел Вы можете назвать?
8. Перечислите основные характеристики, достоинства и недостатки каждого из рассмотренных в данной лекции генераторов псевдослучайных чисел.

Практическая работа № 19

Тема: *Методы генерации ПСЧ*

Практическая работа № 20
Тема: Применение методов генерации ПСЧ

Тема 3.1 Кодирование информации. Компьютеризация шифрования.
Вопросы для устного опроса

1. Кодирование информации. Символьное кодирование. Смысловое кодирование.
2. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.
3. Компьютеризация шифрования. Аппаратное и программное шифрование.
4. Стандартизация программно-аппаратных криптографических систем и средств.
5. Современные программные и аппаратные криптографические средства.

Практическая работа № 21
Тема: Кодирование информации
Практическая работа № 22
Тема: *Исследование информации в двоичном коде в таблице ASCII*
Практическая работа № 23
Тема: *Исследование компьютеризации шифрования*
Практическая работа № 24
Тема: *Программная реализация классических шифров*
Практическая работа № 25
Тема: Изучение реализации классических шифров замены в программе CrypTool или аналоге.
Практическая работа № 26
Тема: Изучение программной реализации классических шифров перестановки.

Тема 3.2 Симметричные системы шифрования
Вопросы для устного опроса

1. Укажите различия между современным и традиционным шифрами с симметричным ключом.
2. Объясните, почему современные блочные шифры спроектированы как шифры подстановки вместо того, чтобы применять шифры транспозиции.
3. Объясните, почему шифр подстановки можно представить себе как шифр транспозиции.
4. Перечислите некоторые компоненты современного блочного шифра.
5. Определите P -блок и перечислите его три варианта. Какой вариант является обратимым?
6. Определите S -блок и покажите необходимое условие обратимости S -блока.
7. Определите составной шифр и перечислите два класса составных шифров.
8. Укажите различие между рассеиванием и перемешиванием
9. Укажите различие между блочным шифром Файстеля и не-Файстеля.
10. Укажите различие между дифференциальным и линейным криптоанализом. Какой из них использует атаку выборки исходного текста? Какой из них использует также атаку знания исходного текста?
11. Укажите различие между синхронным и несинхронным шифрами потока.
12. Определите регистр сдвига с обратной связью и перечислите два варианта, используемые в шифре потока.

Вопросы по стандарту шифрования DES

1. Каков размер блока в DES? Каков размер ключа шифра в DES? Каков размер ключей раунда в DES?
2. Каково число раундов в DES?
3. Сколько смесителей и устройств замены используется в первом способе шифрования и обратного дешифрования? Сколько их используется при втором способе?
4. Сколько перестановок используется в алгоритме шифра DES?
5. Сколько операций ИСКЛЮЧАЮЩЕЕ ИЛИ используется в DES-шифре?
6. Почему DES-функции необходима расширяющая перестановка?
7. Почему генератор ключей раунда нуждается в удалении проверочных бит?
8. Какова разность между слабым ключом, полуслабым ключом и возможно слабым ключом?
9. Что такое двукратный DES? Какая атака двукратного DES сделала его бесполезным?
10. Что такое трехкратный DES? Что такое трехкратный DES с двумя ключами? Что такое трехкратный DES с тремя ключами?

Вопросы по стандарту шифрования AES

1. Перечислите критерии, определенные NIST для AES.
2. Перечислите параметры (размер блока, размер ключа и число раундов) для трех версий AES.
3. Сколько преобразований имеется в каждой версии AES? Сколько ключей необходимо для каждой версии?
4. Сравните DES и AES. Какой из них ориентирован на работу с битом, а какой — на работу с байтом?
5. Определите матрицу состояний в AES. Сколько матриц состояний имеется в каждой версии AES?
6. Какие из четырех преобразований, определенных для AES, изменяют содержание байтов, а какие — не изменяют?
7. Сравните подстановку в DES и AES. Почему мы имеем только одну таблицу перестановки (S -блок) в AES и несколько — в DES?
8. Сравните перестановки в DES и AES. Почему надо иметь расширение и сжатие перестановки в DES и не надо — в AES?
9. Сравните ключи раунда в DES и AES. В каком шифре размер ключа раунда равен размеру блока?
10. Почему смешивающее преобразование (MixColumns) нужно в DES, но не нужно в AES?

Практическая работа № 27

Тема: *Применение режимов работы блочных шифров. Схемы краткого шифрования.*

Практическая работа № 28

Тема: Изучение программной реализации современных симметричных шифров

Практическая работа № 29

Тема: *Исследование общей структурной схемы симметричных криптографических систем.*

Практическая работа № 30

Тема: *Исследование отечественных алгоритмов Магма и Кузнечик*

Практическая работа № 31

Тема: Исследование программной реализации современных симметричных шифров.

Тема 3.3 Ассиметричные системы шифрования

Вопросы для устного опроса

1. Найдите различия между криптосистемами с симметричными ключами и асимметричными ключами.
2. Найдите различия между открытыми и секретными ключами в криптосистеме с асимметричными ключами. Найдите совпадения и различие ключей в криптосистемах с симметричными ключами и с асимметричными ключами.
3. Определите "лазейку" в односторонней функции и объясните её использование в криптографии с асимметричным ключом.
4. Для каких целей может применяться алгоритм RSA?
5. Опишите процесс шифрования с использованием алгоритма RSA.

Практическая работа № 32

Тема: Применение различных асимметричных алгоритмов

Практическая работа № 33

Тема: *Проведение криптоанализа алгоритмов с открытым ключом*

Практическая работа № 34

Тема: Изучение программной реализации асимметричного алгоритма RSA

Тема 3.4 Аутентификация данных. Электронная подпись

Вопросы для устного опроса

1. Аутентификация данных. Общие понятия.
2. Электронная цифровая подпись. Алгоритмы цифровой подписи.
3. MAC.

Практическая работа № 35

Тема: Применение различных функций хеширования

Практическая работа № 36

Тема: Анализ особенностей хешей

Практическая работа № 37

Тема: Применение криптографических атак на хеш-функции

Практическая работа № 38

Тема: *Исследование алгоритма цифровой подписи*

Практическая работа № 39

Тема: Изучение программно-аппаратных средств, реализующих основные функции ЭП

Тема 3.5 Алгоритмы обмена ключей и протоколы аутентификации

Вопросы для устного опроса

1. Для каких целей может применяться алгоритм Диффи-Хеллмана?
2. Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана.
3. Для каких целей может применяться алгоритм Эль-Гамаля?
4. Опишите последовательность действий при использовании алгоритма Эль-Гамаля.
5. Какие атаки возможны при использовании алгоритмов шифрования с открытым ключом?

Практическая работа № 40

Тема: Протокол Диффи-Хеллмана для обмена ключами шифрования

Практическая работа № 41

Тема: Применение протокола Диффи-Хеллмана для обмена ключами шифрования.

Практическая работа № 42

Тема: *Протоколы аутентификации в Windows*

Практическая работа № 43

Тема: *Исследование взаимной аутентификации*

Практическая работа № 44

Тема: *Исследование односторонней аутентификации*

Практическая работа № 45

Тема: Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

Тема 3.6 Криптозащита информации в сетях передачи данных

Вопросы для устного опроса

1. Абонентское шифрование. Пакетное шифрование.
2. Защита центра генерации ключей.
3. Криптомаршрутизатор. Пакетный фильтр.
4. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP

Практическая работа № 46

Тема: *Применение протоколов WPA, WEP для организации безопасного функционирования беспроводной сети.*

Практическая работа № 47

Тема: *Подбор оборудования для реализации проекта беспроводной сети предприятия*

Тема 3.7 Защита информации в электронных платежных системах

Вопросы для устного опроса

1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.
2. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.

Практическая работа № 48

Тема: Применение аутентификации по одноразовым паролям

Практическая работа № 49

Тема: Реализация алгоритмов создания одноразовых паролей

Практическая работа № 50

Тема: *Исследование электронной пластиковые карты и персонального идентификационного номера.*

Практическая работа № 51

Тема: *Применение криптографических протоколов для обеспечения безопасности электронной коммерции.*

Тема 3.8 Компьютерная стеганография

Вопросы для устного опроса

1. Скрытая передача информации в компьютерных системах.
2. Проблема аутентификации мультимедийной информации.
3. Защита авторских прав.

4. Методы компьютерной стеганографии.
5. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.

Практическая работа № 52

Тема: *Исследование скрытой передачи информации в компьютерных системах.*

Практическая работа № 53

Тема: Обзор существующего ПО для встраивания ЦВЗ

Практическая работа № 54

Тема: *Сравнительный анализ существующего ПО для встраивания ЦВЗ.*

Практическая работа № 55

Тема: Реализация простейших стеганографических алгоритмов

3.6 Типовые задания для рубежного контроля по МДК.02.02. Криптографические средства защиты информации

1. Контрольная работа по теме «Криптографические методы защиты информации».

Вариант 1

Ответьте на поставленные вопросы

1. Делимость чисел. Признаки делимости. Простые и составные числа. Алгоритм Евклида для нахождения НОД.
2. Методы симметричного шифрования.
3. Основные методы криптоанализа. Криптографические атаки.

Вариант 2

Ответьте на поставленные вопросы

1. Проверка чисел на простоту. Алгоритмы генерации простых чисел.
2. Методы асимметричного шифрования.
3. Кодирование информации. Символьное кодирование. Смысловое кодирование.

Критерии оценки

Оценкой «отлично» оцениваются ответы, которые показывают прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, давать аргументированные ответы, приводить примеры.

Оценкой «хорошо» оцениваются ответы, обнаруживающие прочные знания основных понятий и задач изучаемой дисциплины, отличаются глубиной и полнотой раскрытия вопросов; владение терминологическим аппаратом; умение давать определения, описывать последовательность технологий материалов, их особенности, делать выводы и обобщения, приводить примеры. Однако допускаются две-три неточности в ответах.

Оценкой «удовлетворительно» оцениваются ответы, свидетельствующие в основном о знании материалов, их свойств, технологий, но отличающиеся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа тем изучаемой дисциплины, недостаточным умением давать аргументированные ответы и приводить примеры. Допускается несколько ошибок в содержании ответа.

Оценкой «неудовлетворительно» оцениваются ответы, обнаруживающие незнание материалов, их свойств, технологий изучаемой предметной области, отличающиеся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными

навыками анализа тем изучаемой дисциплины; неумением давать аргументированные ответы. Допускаются серьезные ошибки в содержании ответов.

2. Тест по теме «Основы криптографии»

1. Шифрование – это…

А) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

Б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

В) удобная среда для вычисления конечного пользователя

2. Кодирование – это…

А) преобразование обычного, понятного текста в код

Б) преобразование

В) написание программы

3. Что требуется для восстановления зашифрованного текста

А) ключ

Б) матрица

В) вектор

4. Когда появилось шифрование

А) четыре тысячи лет назад

Б) две тысячи лет назад

В) пять тысяч лет назад

5. Первым известным применением шифра считается

А) египетский текст

Б) русский

В) нет правильного ответа

6. Какую секретную информацию хранит Windows

А) пароли для доступа к сетевым ресурсам

Б) пароли для доступа в Интернет

В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

7. Алфавит – это…

А) конечное множество используемых для кодирования информации знаков

Б) буквы текста

В) нет правильного ответа

8. Текст – это…

А) упорядоченный набор из элементов алфавита

Б) конечное множество используемых для кодирования информации знаков

В) все правильные

9. Примеры алфавитов:

А) Z_{256} – символы, входящие в стандартные коды ASCII и КОИ-8

Б) восьмеричный и шестнадцатеричный алфавиты

В) АЕЕ

10. Шифрование – это…

А) преобразовательный процесс исходного текста в зашифрованный

Б) упорядоченный набор из элементов алфавита

В) нет правильного ответа

11. Дешифрование – это…

А) на основе ключа шифрованный текст преобразуется в исходный

Б) пароли для доступа к сетевым ресурсам

В) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере

12. Криптографическая система представляет собой…

А) семейство T преобразований открытого текста, члены его семейства индексируются символом k

Б) программу

В) систему

13. Пространство ключей k – это…

А) набор возможных значений ключа

Б) длина ключа

В) нет правильного ответа

14. Криптосистемы разделяются на:

А) симметричные

Б) ассиметричные

В) с открытым ключом

15. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования

А) 1

Б) 2

В) 3

16. Сколь ключей используется в системах с открытым ключом

А) 2

Б) 3

В) 1

17. Какие ключи используются в системах с открытым ключом

А) открытый

Б) закрытый

В) нет правильного ответа

18. Как связаны ключи друг с другом в системе с открытым ключом

А) математически

Б) логически

В) алгоритмически

19. Электронной подписью называется…

А) присоединяемое к тексту его криптографическое преобразование

Б) текст

В) зашифрованный текст

20. Криптостойкость – это…

А) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа

Б) свойство гаммы

В) все ответы верны

21. Показатели криптостойкости:

А) количество всех возможных ключей

Б) среднее время, необходимое для криптоанализа

В) количество символов в ключе

22. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

А) знание алгоритма шифрования не должно влиять на надежность защиты

Б) структурные элементы алгоритма шифрования должны быть неизменными

В) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования

23. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

А) длина шифрованного текста должна быть равной лине исходного текста

Б) зашифрованное сообщение должно поддаваться чтению только при наличии ключа

В) нет правильного ответа

24. Основные современные методы шифрования:

А) алгоритма гаммирования

Б) алгоритмы сложных математических преобразований

В) алгоритм перестановки

25. Символы исходного текста складываются с символами некой случайной последовательности – это…

А) алгоритм гаммирования

Б) алгоритм перестановки

В) алгоритм аналитических преобразований

26. Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…

А) алгоритм перестановки

Б) алгоритм подстановки

В) алгоритм гаммирования

27. Самой простой разновидность подстановки является

А) простая замена

Б) перестановка

В) простая перестановка

28. Из скольких последовательностей состоит расшифровка текста по таблице Вижинера

А) 3

Б) 4

В) 5

29. Какие таблицы Вижинера можно использовать для повышения стойкости шифрования

А) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке

Б) в качестве ключа используется случайность последовательных чисел

В) нет правильного ответа

30. В чем суть метода перестановки

А) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов

Б) замена алфавита

В) все правильные

31. Сколько существует способов гаммирования

А) 2

Б) 5

В) 3

32. Чем определяется стойкость шифрования методом гаммирования

А) свойством гаммы

Б) длина ключа

В) нет правильного ответа

33. Что может использоваться в качестве гаммы

А) любая последовательность случайных символов

Б) число

В) все ответы верны

34. Какой метод используется при шифровании с помощью аналитических преобразований

А) алгебры матриц

Б) матрица

В) факториал

35. Что используется в качестве ключа при шифровании с помощью аналитических преобразований

А) матрица А

Б) вектор

В) обратная матрица

36. Как осуществляется дешифрование текста при аналитических преобразованиях

А) умножение матрицы на вектор

Б) деление матрицы на вектор

В) перемножение матриц

37. Комбинации комбинированного метода шифрования:

А) подстановка+гаммирование

Б) гаммирование+гаммирование

В) подстановка+перестановка

38. Для чего использовался DES-алгоритм из-за небольшого размер ключа

А) закрытия коммерческой информации

Б) шифрования секретной информации

В) нет правильного ответа

39. Основные области применения DES-алгоритма

А) хранение данных на компьютере

Б) электронная система платежей

В) аутентификация сообщений

40. Когда был введен в действие ГОСТ 28147-89

А) 1990

Б) 1890

В) 1995

41. Достоинства ГОСТа 28147-89

А) высокая стойкость

Б) цена

В) гибкость

42. Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма

А) отсутствием начальной перестановки и числом циклов шифрования

Б) длиной ключа

В) методом шифрования

43. Ключ алгоритма ГОСТ – это…

А) массив, состоящий из 32-мерных векторов

Б) последовательность чисел

В) алфавит

44. Какой ключ используется в шифре ГОСТ

А) 256-битовый

Б) 246-битовый

В) 356-битовый

45. Примеры программных шифраторов:

А) PGP

Б) BestCrypt 6.04

В) PTR

46. Плюсы программных шифраторов:

А) цена

Б) гибкость

В) быстродействие

47. УКЗД – это…

А) устройство криптографической защиты данных

Б) устройство криптографической заданности данных

В) нет правильного ответа

48. Блок управления – это…

А) основной модуль шифратора, который «заведует» работой всех остальных

Б) устройство криптографической заданности данных

В) проходной шифратор

49. Вычислитель – это…

А) набор регистров, сумматоров, блоков подстановки, связанных собой шинами передачи данных

Б) файлы, использующие различные методы кэширования

В) язык описания данных

50. Блок управления – это…

А) аппаратно реализованная программа, управляющая вычислителем

Б) язык описания данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

51. Какой шифратор можно использовать для защиты передаваемой в Сеть информации

А) обычный шифратор

Б) проходной шифратор

В) табличный шифратор

52. Египетский текст дотировался примерно…

А) 1900 г. д. н.э.

Б) 1890 г. д. н.э.

В) 1990 г.

53. Один из самых известных методов шифрования носит имя…

А) Цезаря
Б) Гейца
В) Вижинера

54. Из каких структурных единиц состоит шифропроцессор
А) вычислитель
Б) блок управления
В) буфер ввода-вывода

55. Криптографические действия выполняет…
А) вычислитель
Б) буфер ввода-вывода
В) блок управления

56. Наиболее известные разновидности полиалфавита:
А) одноконтурные
Б) многоконтурные
В) поликонтурные

57. Зашифрованный файл, хранящийся на логическом диске, который подключается к системе как еще один логический диск – это…
А) виртуальный контейнер
Б) файл
В) программа

58. Устройство, дающее статически случайный шум – это…
А) генератор случайных чисел
Б) контроль ввода на компьютер
В) УКЗД

59. Какие дополнительные порты ввода-вывода содержит УКЗД:
А) COM
Б) USB
В) FGR

60. Сколько существует перестановок в стандарте DES
А) 3
Б) 4
В) 2

61. Какие перестановки существуют в стандарте DES
А) простые
Б) расширенные
В) сокращенные

62. Как называется модификация DESa
А) Triple Des
Б) M-506
В) Deh

3.7 Типовые задания для промежуточного контроля по МДК.02.02. Криптографические средства защиты информации

Экзаменационные вопросы

1. Предмет и задачи криптографии. История криптографии. Основные термины.
2. Элементы теории множеств. Группы, кольца, поля.
3. Делимость чисел. Признаки делимости. Простые и составные числа.
4. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.
5. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.
6. Классы. Полная и приведенная система вычетов. Функция Эйлера.
7. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.
8. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.
9. Китайская теорема об остатках.
10. Проверка чисел на простоту. Алгоритмы генерации простых чисел.
11. Метод пробных делений. Решето Эратосфена.
12. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма.
1. Метод Полларда.
13. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.
14. Арифметические операции над большими числами.
15. Эллиптические кривые и их приложения в криптографии.
16. Классификация основных методов криптографической защиты. Методы симметричного шифрования
17. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.
18. Методы перестановки. Табличная перестановка, маршрутная перестановка
19. Гаммирование. Гаммирование с конечной и бесконечной гаммами
20. Основные методы криптоанализа. Криптографические атаки.
21. Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Кирхгоффа.
22. Перспективные направления криптоанализа, квантовый криптоанализ.
23. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.
24. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.
25. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.
26. Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.
27. Изучение современных программных и аппаратных криптографических средств.
28. Общие сведения. Структурная схема симметричных криптографических систем
29. Отечественные алгоритмы Магма, Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.
30. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4
31. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.
32. Элементы теории чисел в криптографии с открытым ключом.

33. Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи
34. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.
35. Взаимная аутентификация. Односторонняя аутентификация
36. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.
37. Криптомаршрутизатор. Пакетный фильтр
38. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.
39. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер
40. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.
41. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.
42. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ

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.

3.8 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. Требования по защите персональных данных
3. Требования по защите конфиденциальных данных предприятия
4. Системы контроля и управления доступом на предприятии
5. Способы ограничения доступа к информации
6. Признаки наличия вредоносного программного обеспечения
7. Средства защиты информации в компьютерных сетях
8. Средства обнаружения компьютерных атак
9. Способы предупреждения компьютерных атак
10. Программно-аппаратные средства уничтожения информации и носителей информации

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

4.1 Паспорт

Экзамен предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Условием допуска к экзамену являются положительные аттестации: по промежуточной аттестации МДК.02.01 и МДК.02.02; по учебной практике УП.02; по производственной практике ПП.02.

Результаты освоения модуля, подлежащие проверке на 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.2.1., ПК. 2.2., ПК.2.3., ПК 2.4., ПК 2.5., ПК 2.6.

4.2 Задания для экзаменующегося

Инструкция: внимательно прочитайте задание. Время выполнения задания – 30 минут

Текст задания №1:

Вариант № 1

Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны? Предложите технологию учета и отработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудования «Сервис-ТЕХНО».

Вариант № 2

Опишите технологический процесс обработки информации. Перечислите и охарактеризуйте технологические процессы процесса обработки информации. Какие режимы обработки информации вам известны? Перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Вариант № 3

Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте

действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Вариант № 4

Опишите параметры локальной политики безопасности операционной системы Windows, параметры и значения параметров Политики учетной записи, параметры и значения параметров Политики паролей. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль.

Вариант № 5

Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера. Предложите стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Вариант № 6

Опишите параметры и значения параметров Политики аудита. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале? Включите аудит успеха и отказа всех параметров.

Вариант № 7

Опишите причины возникновения остаточной информации.

Приведите примеры устройств уничтожения информации с магнитных носителей. Перечислите основные требования к современным устройствам уничтожения информации с магнитных носителей. Охарактеризуйте программные методы уничтожения информации. Обоснуйте выбор устройства уничтожения информации с магнитных носителей.

Вариант № 8

Проведите анализ защищенности заданного объекта защиты информации по следующим разделам: виды возможных угроз, характер происхождения угроз, классы каналов несанкционированного получения информации, источники появления угроз, причины нарушения целостности информации, потенциально возможные злоумышленные действия.

Вариант № 9

Опишите разделы реестра Windows. В каких разделах реестра хранится информация о выбранной политике безопасности? Опишите возможности программы REGEDIT.EXE. Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

Вариант № 10

Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту: ячейки для

ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

Текст задания №2:

Инструкция: внимательно прочитайте задание. Время выполнения задания – 30 минут
Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания.

Вариант № 1

Описать простейшие стеганографические алгоритмы. Выбрать контейнер и выполнить внедрение в него некоторой информации. От чего зависит криптостойкость стеганографических систем?

Вариант № 2.

Опишите последовательность действий при использовании алгоритма Диффи-Хеллмана. Для каких целей может применяться алгоритм Диффи-Хеллмана? На чём основывается безопасность обмена ключа по схеме Диффи-Хеллмана?

Вариант № 3.

Приведите алгоритм реализации цифровой подписи RSA. В чем отличие подписи RSA от алгоритма шифрования RSA? Приведите примеры программно-аппаратных средств, реализующих основные функции электронной цифровой подписи.

Вариант № 4.

Представьте алгоритм работы российского стандарта шифрования ГОСТ 28147-89. Выполнить ручное шифрование исходного текста с помощью алгоритма ГОСТ 28147-89. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES. Приведите примеры программ симметричного шифрования.

Вариант № 5.

Перечислите классические алгоритмы шифрования, которые описаны и реализованы в программе CrypTool. Зашифруйте и расшифруйте сообщение с помощью одного из имеющегося в программе CrypTool классического шифра замены и шифра перестановки.

Вариант № 6.

Приведите алгоритм шифрования текста методом гаммирования. Зашифруйте и расшифруйте сообщение по представленному алгоритму. Опишите особенности двоичного гаммирования.

Вариант № 7.

Приведите алгоритм шифрования текста методом перестановки. Зашифруйте и расшифруйте сообщение по представленному алгоритму. Приведите примеры классических методов шифрования.

Вариант № 8.

Приведите алгоритм шифрования текста методом замены. Зашифруйте и расшифруйте сообщение по представленному алгоритму. Приведите примеры классических методов шифрования. Опишите сходства и различия шифра Гронсфельда и шифра Цезаря.

Вариант № 9.

Опишите методику криптоанализа, основанную на исследовании частотности закрытого текста. Исследуйте частотность зашифрованного текста. Приведите типовые методы криптоанализа классических алгоритмов.

Вариант № 10.

Составить алгоритм шифрования и расшифрования методом Виженера. Оцените криптостойкость данного метода шифрования

4.3 Пакет экзаменатора

Условия выполнения задания:

Время выполнения каждого задания 30 минут. Обучающиеся могут воспользоваться ПК и необходимым программным обеспечением для выполнения задания.

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.