Автономная некоммерческая организация высшего образования
«Российский новый университет»
Колледж

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по профессиональному модулю

ПМ.01. Защита информации в автоматизированных системах программными и программно-аппаратными средствами

для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем

(базовая подготовка)
на базе среднего общего образования

Москва 2020

Одобрена
предметной (цикловой)
комиссией по специальности
09.02.05 Прикладная
информатика (по отраслям)

Протокол № 04
от «03» декабря 2020 г.

Разработана на основе Федерального государственного образовательного стандарта для специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553, и учебного плана программы подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Председатель предметной (цикловой) комиссии:

_____/ Аскерова В.И.

Заместитель директора по учебно-методической работе:

_____/ Харчевникова Е.М.

Составители (авторы): Шарапова Л.В., ст. преподаватель кафедры информационных технологий и естественнонаучных дисциплин,
Пиков В.А., ст. преподаватель кафедры телекоммуникационных систем и информационной безопасности

Рецензент: Киркорова Н.И., генеральный директор ООО «Кибит», кандидат экономических наук, доцент

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

В результате освоения профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» обучающийся должен обладать предусмотренными ФГОС по программе подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» следующими умениями, знаниями, общими и профессиональными компетенциями:

У1 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У2 - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

У3 - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У4 - применять программные и программно-аппаратные средства для защиты информации в базах данных;

У5 - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У6 - применять математический аппарат для выполнения криптографических преобразований;

У7 - использовать типовые программные криптографические средства, в том числе электронную подпись;

У8 - применять средства гарантированного уничтожения информации;

У9 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У10 - осуществлять 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;

З1 - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З2 - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З3 - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З4 - основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З5 - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З6 - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

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

ОК 0 2 - Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03 - Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 0 4 - Работать в коллективе и команде, эффективно взаимодействовать с коллегами,
руководством, клиентами.

ОК 0 5 - Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 0 6 - Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 0 7 - Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 10 - Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1 - Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2 - Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3 - Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4 - Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5 - Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

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.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

В результате аттестации по учебной дисциплине «МДК.02.01. Программные и программно-аппаратные средства защиты информации» осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Результаты обучения: умения, знания, профессиональные и общие компетенции	Показатели оценки результата	Форма контроля и оценивания
Уметь:		
У1 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Установка, настройка, применение программных и программно-аппаратных средств защиты информации	Экспертная оценка результатов деятельности обучающихся при выполнении практических работ: Практическая работа № 1 «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 «Обзор стандартов. Работа с содержанием стандартов». Практическая работа № 3 «Учет, обработка, хранение и передача информации в АИС». Практическая работа № 4 «Ограничение доступа на вход в систему». Практическая работа № 5 «Идентификация и аутентификация пользователей». Практическая работа № 6 «Разграничение доступа». Практическая работа № 7 «Регистрация событий (аудит)». Практическая работа № 8 «Контроль целостности данных». Практическая работа № 9 «Уничтожение остаточной информации». Практическая работа № 10 «Управление политикой безопасности». Практическая работа № 11 «Криптографическая защита. Обзор программ шифрования
У2 - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями	Умение устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями	
У3 - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации	Выполнение диагностики, устранение отказов, обеспечение работоспособности и тестирование функций программно-аппаратных средств защиты информации	
У4 - применять программные и программно-аппаратные средства для защиты информации в базах данных	Демонстрация умения применять программные и программно-аппаратные средства для защиты информации в базах данных	
У5 - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Умение проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	
У6 - применять математический аппарат для выполнения криптографических преобразований	Применение математического аппарата для выполнения криптографических преобразований	
У7 - использовать типовые программные криптографические средства, в том числе электронную подпись	Использование типовых программных криптографических средств, в том числе электронной подписи	
У8 - применять средства гарантированного уничтожения информации	Применение средств гарантированного уничтожения информации	
У9 - устанавливать, настраивать, применять	Умение устанавливать, настраивать, применять	

программные и программно-аппаратные средства защиты информации	программные и программно-аппаратные средства защиты информации	данных». Практическая работа № 12 «Шаблоны безопасности». Практическая работа № 13 «Распределение каналов в соответствии с источниками воздействия на информацию». Практическая работа № 14 «Организация доступа к файлам». Практическая работа № 15 «Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД». Практическая работа № 16 «Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО». Практическая работа № 17 «Защита информации от несанкционированного копирования с использованием специализированных программных средств». Практическая работа № 18 «Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)». Практическая работа № 19 «Применение средства восстановления остаточной информации на примере Foremost или аналога». Практическая работа № 20 «Применение специализированного программного средства для восстановления удаленных файлов». Практическая работа № 21 «Применение программ для безвозвратного удаления данных». Практическая работа № 22 «Применение программ для шифрования данных на съемных носителях». Практическая работа № 23
У10 - осуществлять 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	Демонстрация умения осуществлять 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	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Использование различных источников, включая электронные ресурсы, медиаресурсы, интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	Демонстрация ответственности за принятые решения; обоснованность самоанализа и коррекция результатов собственной работы	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Грамотность устной и письменной речи, ясность формулирования и изложения мыслей	

		«Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений».
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	Практическая работа № 24 «Развертывание VPN».
		Практическая работа № 25 «Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr».
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	Практическая работа № 26 «Изучение различных способов закрытия "опасных" портов».
		Практическая работа № 27 «Изучение механизмов защиты СУБД MS Access».
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	Практическая работа № 28 «Изучение штатных средств защиты СУБД MSSQL Server».
		Практическая работа № 29 «Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов».
ОК 09. Использовать информационные технологии в профессиональной деятельности	Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	Практическая работа № 30 «Проведение аудита ЛВС сетевым сканером».
		Практическая работа № 31 «Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке».
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	Практическая работа № 32 «Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов».
ПК 2.1 - Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	Практическая работа № 33 «Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других
ПК 2.2 - Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными	

ПК 2.3 - Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации ПК 2.4 - Осуществлять обработку, хранение и передачу информации ограниченного доступа ПК 2.5 - Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств 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	средствами Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	аналогов». Практическая работа № 34 «Изучение типовых решений для построения VPN на примере VipNet или других аналогов». Практическая работа № 35 «Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов». Практическая работа № 36 «Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов» Контрольная работа № 1 «Защита информационных систем» Проведение экзамена
Знать:		
З1 - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Правильность определения особенностей и способов применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль)
З2 - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Знание методов тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль)
З3 - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	Правильность определения типовых моделей управления доступом, средств, методов и протоколов идентификации и аутентификации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль)

З4 - основные понятия криптографии и типовых криптографических методов и средств защиты информации	Правильность определения основных понятий криптографии и типовых криптографических методов и средств защиты информации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль)
З5 - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Знание особенностей и способов применения программных и программно-аппаратных средств гарантированного уничтожения информации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль)
З6 - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Знание типовых средств и методов ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль)

В результате аттестации по учебной дисциплине «МДК.02.02. Криптографические средства защиты информации» осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Результаты обучения: умения, знания, профессиональные и общие компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Уметь:		
У1 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации У2 - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями У3 - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации У4 - применять программные и программно-аппаратные	Установка, настройка, применение программных и программно-аппаратных средств защиты информации Умение устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями Выполнение диагностики, устранение отказов, обеспечение работоспособности и тестирование функций программно-аппаратных средств защиты информации Демонстрация умения применять программные и	Экспертная оценка результатов деятельности обучающихся при выполнении практических работ: Практическая работа № 37 «Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений». Практическая работа № 38 «Проверка чисел на простоту». Практическая работа № 39 «Решение задач с элементами теории чисел». Практическая работа № 40 «Применение классических шифров замены». Практическая работа № 41 «Применение классических

средства для защиты информации в базах данных	программно-аппаратные средства для защиты информации в базах данных	шифров перестановки». Практическая работа № 42 «Применение метода гаммирования».
У5 - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Умение проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации	Практическая работа № 43 «Криптоанализ шифра простой замены методом анализа частотности символов». Практическая работа № 44 «Криптоанализ классических шифров методом полного перебора ключей».
У6 - применять математический аппарат для выполнения криптографических преобразований	Применение математического аппарата для выполнения криптографических преобразований	Практическая работа № 45 «Криптоанализ шифра Виженера». Практическая работа № 46 «Применение методов генерации ПСЧ».
У7 - использовать типовые программные криптографические средства, в том числе электронную подпись	Использование типовых программных криптографических средств, в том числе электронной подписи	Практическая работа № 47 «Кодирование информации». Практическая работа № 48 «Программная реализация классических шифров».
У8 - применять средства гарантированного уничтожения информации	Применение средств гарантированного уничтожения информации	Практическая работа № 49 «Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге».
У9 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Умение устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации	Практическая работа № 50 «Изучение программной реализации современных симметричных шифров».
У10 - осуществлять 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	Демонстрация умения осуществлять 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	Практическая работа № 51 «Применение различных асимметричных алгоритмов». Практическая работа № 52 «Изучение программной реализации асимметричного алгоритма RSA». Практическая работа № 53 «Применение различных функций хеширования, анализ особенностей хешей».
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Практическая работа № 54 «Применение криптографических атак на хеш-функции». Практическая работа № 55 «Изучение программно-аппаратных средств, реализующих основные функции ЭП».
ОК 02. Осуществлять поиск, анализ и интерпретацию	Использование различных источников, включая	Практическая работа № 56 «Применение протокола

информации, необходимой для выполнения задач профессиональной деятельности	электронные ресурсы, медиаресурсы, интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Диффи - Хеллмана для обмена ключами шифрования». Практическая работа № 57 «Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos». Практическая работа № 58 «Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей». Практическая работа № 59 «Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ». Практическая работа № 60 «Реализация простейших стеганографических алгоритмов». Контрольная работа № 1 «Криптографические методы защиты информации» Проведение экзамена
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	Демонстрация ответственности за принятые решения; обоснованность самоанализа и коррекция результатов собственной работы	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Грамотность устной и письменной речи, ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	

ОК 09. Использовать информационные технологии в профессиональной деятельности	Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ПК 2.1 - Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	
ПК 2.2 - Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	
ПК 2.3 - Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	
ПК 2.4 - Осуществлять обработку, хранение и передачу информации ограниченного доступа	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	
ПК 2.5 - Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	
ПК 2.6 - Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных	

программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	
Знать:		
З1 - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Правильность определения особенностей и способов применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль) Оценка защиты самостоятельной работы СРС № 1-8
З2 - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Знание методов тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль) Оценка защиты самостоятельной работы СРС № 1-8
З3 - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации	Правильность определения типовых моделей управления доступом, средств, методов и протоколов идентификации и аутентификации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль) Оценка защиты самостоятельной работы СРС № 1-8
З4 - основные понятия криптографии и типовых криптографических методов и средств защиты информации	Правильность определения основных понятий криптографии и типовых криптографических методов и средств защиты информации	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль) Оценка защиты самостоятельной работы СРС № 1-8
З5 - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	Знание особенностей и способов применения программных и программно-аппаратных средств гарантированного уничтожения	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса;

	информации	контрольной работы № 1 (рубежный контроль) Оценка защиты самостоятельной работы СРС № 1-8
З6 - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Знание типовых средств и методов ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа	Экспертная оценка результатов деятельности обучающихся при выполнении текущего контроля, устного опроса; контрольной работы № 1 (рубежный контроль) Оценка защиты самостоятельной работы СРС № 1-8

3 ОЦЕНКА ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по профессиональному модулю, направленные на формирование общих и профессиональных компетенций.

Оценка знаний и умений предусматривает проведение устного опроса, самостоятельной работы студента, практических работ при текущем контроле, контрольной работы при рубежном контроле, ответы на теоретические вопросы, выполнение практической работы при промежуточной аттестации.

Контроль и оценка освоения учебной дисциплины МДК.02.01. «Программные и программно-аппаратные средства защиты информации» по темам (разделам)

Элемент учебной дисциплины	Формы и методы контроля					
	Текущий контроль		Рубежный контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Устный опрос	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 1.2. Стандарты безопасности	Устный опрос. Практические работы № 1-2	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 1.3. Защищенная автоматизированная система	Устный опрос. Практические работы № 3-11	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Практические работы № 12	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 1.4. Дестабилизирующее	Устный опрос. Практическая работа № 13	ОК 01-ОК 10 ПК 2.1		ОК 01-ОК 10 ПК 2.1	Экзамен	ОК 01-ОК 10 ПК 2.1

воздействие на объекты защиты		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Устный опрос. Практические работы № 14-15	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.1. Основы защиты автономных автоматизированных систем	Устный опрос	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.2. Защита программ от изучения	Устный опрос	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.3. Вредоносное программное	Устный опрос. Практическая работа № 16	ОК 01-ОК 10 ПК 2.1 ПК 2.2		ОК 01-ОК 10 ПК 2.1 ПК 2.2	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2

обеспечение		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.4. Защита программ и данных от несанкционированного копирования	Устный опрос. Практические работы № 17-18	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.5. Защита информации на машинных носителях	Устный опрос. Практические работы № 19-21	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Практические работы № 22	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	Устный опрос	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.7. Системы обнаружения атак и вторжений	Устный опрос. Практическая работа № 23	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3

		ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.1. Основы построения защищенных сетей	Устный опрос	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.2. Средства организации VPN	Устный опрос. Практическая работа № 24	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Устный опрос. Практические работы № 25-26	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 4.2. Защита информации в базах данных	Устный опрос. Практические работы № 27	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4	Практические работы №28	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4

		ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 5.1. Мониторинг систем защиты	Устный опрос. Практические работы № 29-30	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 5.2. Изучение мер защиты информации в информационных системах	Устный опрос. Практическая работа № 31	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Контрольная работа № 1	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 5.3. Изучение современных программно-аппаратных комплексов	Устный опрос. Практические работы № 32-36	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6

Контроль и оценка освоения учебной дисциплины МДК.02.02«Криптографические средства защиты информации» по темам (разделам)

Элемент учебной дисциплины	Формы и методы контроля					
	Текущий контроль		Рубежный контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З
Тема 1.1. Введение. Математические основы криптографии	Устный опрос. Практические работы № 37-39.	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.1. Методы криптографической защиты информации	Устный опрос. Практические работы № 40-42.	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	Контрольная работа № 1	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.2. Криптоанализ	Устный опрос. Практические работы № 43-45.	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 2.3. Поточные шифры и	Устный опрос. Практическая работа № 46	ОК 01-ОК 10 ПК 2.1		ОК 01-ОК 10 ПК 2.1	экзамен	ОК 01-ОК 10 ПК 2.1

генераторы псевдослучайных чисел		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.1. Кодирование информации. Компьютеризация шифрования	Устный опрос. Практические работы № 47-49.	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.2. Симметричные системы шифрования	Устный опрос. Практическая работа № 50	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.3. Асимметричные системы шифрования	Устный опрос. Практические работы № 51-52	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.4. Аутентификация данных. Электронная	Устный опрос. Практические работы № 53-54	ОК 01-ОК 10 ПК 2.1 ПК 2.2	Практические работы № 55	ОК 01-ОК 10 ПК 2.1 ПК 2.2	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2

подпись		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Устный опрос. Практические работы № 56-57	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.6. Криптозащита информации в сетях передачи данных	Устный опрос.	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.7. Защита информации в электронных платежных системах	Устный опрос. Практическая работа № 58.	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6
Тема 3.8. Компьютерная стеганография	Устный опрос. Практические работы № 59	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3	Практические работы № 60	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3

		ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6		ПК 2.4 ПК 2.5 ПК 2.6 У1-У10 З1-З6

3.2 Контрольно-оценочные средства (КОС) для текущего контроля знаний, умений обучающихся

3.2.1 Контрольно-оценочные средства (КОС) для текущего контроля знаний, умений, обучающихся по учебной дисциплине МДК.02.01 «Программные и программно-аппаратные средства защиты информации»

Типовые задания для оценки знаний З1, З2, З3, З4, З5, З6, умений У1, У2, У3, У4, У5, У6, У7, У8, У9, У10 (текущий контроль)

Тема 1.1 Предмет и задачи программно-аппаратной защиты информации.

1. Задание для устного опроса по темам

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

Критерии оценки

«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.

«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 и др.

«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.

«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.

Тема 1.2 Стандарты безопасности.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 1 «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».

Выполнение практической работы № 2 «Обзор стандартов. Работа с содержанием стандартов».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 1.3 Защищенная автоматизированная система.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 3 «Учет, обработка, хранение и передача информации в АИС».

Выполнение практической работы № 4 «Ограничение доступа на вход в систему».

Выполнение практической работы № 5 «Идентификация и аутентификация пользователей».

Выполнение практической работы № 6 «Ограничение доступа на вход в систему».

Выполнение практической работы № 7 «Регистрация событий (аудит)».

Выполнение практической работы № 8 «Контроль целостности данных».

Выполнение практической работы № 9 «Уничтожение остаточной информации».

Выполнение практической работы № 10 «Управление политикой безопасности».

Выполнение практической работы № 11 «Криптографическая защита. Обзор программ шифрования данных».

Выполнение практической работы № 12 «Шаблоны безопасности».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 1.4 Дестабилизирующее воздействие на объекты защиты.

1. Задание для устного опроса по темам

1. Источники дестабилизирующего воздействия на объекты защиты.
2. Способы воздействия на информацию.
3. Причины и условия дестабилизирующего воздействия на информацию.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 13 «Распределение каналов в соответствии с источниками воздействия на информацию».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 1.5 Принципы программно-аппаратной защиты информации от несанкционированного доступа.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 14 «Организация доступа к файлам».

Выполнение практической работы № 15 «Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 2.1 Основы защиты автономных автоматизированных систем.

1. Задание для устного опроса по темам

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. Понятие АМДЗ (доверенная загрузка).
5. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.

Критерии оценки

«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.

«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 и др.

«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.

«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.

Тема 2.2 Защита программ от изучения.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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.

Тема 2.3 Вредоносное программное обеспечение.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 16 «Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 2.4 Защита программ и данных от несанкционированного копирования.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 17 «Защита информации от несанкционированного копирования с использованием специализированных программных средств».

Выполнение практической работы № 18 «Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 2.5 Защита информации на машинных носителях.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 19 «Применение средства восстановления остаточной информации на примере Foremost или аналога».

Выполнение практической работы № 20 «Применение специализированного программного средства для восстановления удаленных файлов».

Выполнение практической работы № 21 «Применение программ для безвозвратного удаления данных».

Выполнение практической работы № 22 «Применение программ для шифрования данных на съемных носителях».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 2.6 Аппаратные средства идентификации и аутентификации пользователей.

1. Задание для устного опроса по темам

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

Критерии оценки

«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.

«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 и др.

«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.

«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.

Тема 2.7 Системы обнаружения атак и вторжений.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 23 «Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 3.1 Основы построения защищенных сетей.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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.

Тема 3.2 Средства организации VPN.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 24 «Развертывание VPN».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 4.1 Обеспечение безопасности межсетевого взаимодействия.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 25 «Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr».

Выполнение практической работы № 26 «Изучение различных способов закрытия "опасных" портов».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 4.2 Защита информации в базах данных.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 27 «Изучение механизмов защиты СУБД MS Access».

Выполнение практической работы № 28 «Изучение штатных средств защиты СУБД MSSQL Server».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 5.1 Мониторинг систем защиты.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 29 «Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов».

Выполнение практической работы № 30 «Проведение аудита ЛВС сетевым сканером».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 5.2 Изучение мер защиты информации в информационных системах.

1. Задание для устного опроса по темам

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

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 31 «Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Тема 5.3 Изучение современных программно-аппаратных комплексов.

1. Задание для устного опроса по темам

1. Характеристика современных программно-аппаратных комплексов.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 32 «Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов».

Выполнение практической работы № 33 «Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов».

Выполнение практической работы № 34 «Изучение типовых решений для построения VPN на примере VipNet или других аналогов».

Выполнение практической работы № 35 «Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов».

Выполнение практической работы № 36 «Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению лабораторных работ по МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Типовые задания для оценки знаний З1, З2, З3, З4, З5, З6, умений У1, У2, У3, У4, У5, У6, У7, У8, У9, У10 (рубежный контроль)

1. Задание для устного опроса по темам

Контрольная работа № 1 «Защита информационных систем».

Цель: проверить теоретические знания и практические навыки по темам дисциплины МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Задание. Ответить на поставленные вопросы

Вариант 1

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

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 оценки

Отметкой «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.

Отметкой «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.

Отметкой «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.

Отметкой «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.

3.2.2 Контрольно-оценочные средства (КОС) для текущего контроля знаний, умений, обучающихся по учебной дисциплине МДК.02.02 «Криптографические средства защиты информации»

Типовые задания для оценки знаний З1, З2, З3, З4, З5, З6, умений У1, У2, У3, У4, У5, У6, У7, У8, У9, У10 (текущий контроль)

Тема 1.1 Введение. Математические основы криптографии

1. Задание для устного опроса по темам

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. Теорема Ферма - Эйлера. Алгоритм быстрого возведения в степень по модулю.

7. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.

8. Китайская теорема об остатках.

9. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.

10. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.

11. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.

12. Арифметические операции над большими числами.

13. Эллиптические кривые и их приложения в криптографии.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 37 «Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений».

Выполнение практической работы № 38 «Проверка чисел на простоту».

Выполнение практической работы № 39 «Решение задач с элементами теории чисел».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 1. Подготовка доклада-сообщения на тему: «История криптографии».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 2.1 Методы криптографической защиты информации.

1. Задание для устного опроса по темам

1. Классификация основных методов криптографической защиты. Методы симметричного шифрования.
2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.
3. Методы перестановки. Табличная перестановка, маршрутная перестановка.
4. Гаммирование. Гаммирование с конечной и бесконечной гаммами.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 40 «Применение классических шифров замены».

Выполнение практической работы № 41 «Применение классических шифров перестановки».

Выполнение практической работы № 42 «Применение метода гаммирования».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 2. Подготовка реферата на тему: «Методы криптографической защиты информации».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 2.2 Криптоанализ

1. Задание для устного опроса по темам

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

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 43 «Криптоанализ шифра простой замены методом анализа частотности символов».

Выполнение практической работы № 44 «Криптоанализ классических шифров методом полного перебора ключей».

Выполнение практической работы № 45 «Криптоанализ шифра Виженера».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 3. Подготовка реферата на тему: «Основные методы криптоанализа».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 2.3 Поточные шифры и генераторы псевдослучайных чисел

1. Задание для устного опроса по темам

1. Основные принципы поточного шифрования.
2. Применение генераторов ПСЧ в криптографии.
3. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 46 «Применение методов генерации ПСЧ».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

Тема 3.1 Кодирование информации. Компьютеризация шифрования

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 47 «Кодирование информации».

Выполнение практической работы № 48 «Программная реализация классических шифров».

Выполнение практической работы № 49 «Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 4. Подготовка компьютерной презентации на тему: «Современные программные и аппаратные криптографические средства».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 3.2 Симметричные системы шифрования

1. Задание для устного опроса по темам

1. Общие сведения. Структурная схема симметричных криптографических систем.

2. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

3. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 50 «Изучение программной реализации современных симметричных шифров».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

Тема 3.3 Асимметричные системы шифрования

1. Задание для устного опроса по темам

1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.

2. Элементы теории чисел в криптографии с открытым ключом.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 51 «Применение различных асимметричных алгоритмов».

Выполнение практической работы № 52 «Изучение программной реализации асимметричного алгоритма RSA».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

Тема 3.4 Аутентификация данных. Электронная подпись

1. Задание для устного опроса по темам

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

4. Однонаправленные хеш-функции.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 53 «Применение различных функций хеширования, анализ особенностей хешей».

Выполнение практической работы № 54 «Применение криптографических атак на хеш-функции».

Выполнение практической работы № 55 «Изучение программно-аппаратных средств, реализующих основные функции ЭП».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 5. Подготовка доклада-сообщения на тему: «Основы построения электронной цифровой подписи».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 3.5 Алгоритмы обмена ключей и протоколы аутентификации

1. Задание для устного опроса по темам

1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем.
2. Протоколы аутентификации.
3. Взаимная аутентификация. Односторонняя аутентификация.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 56 «Применение протокола Диффи-Хеллмана для обмена ключами шифрования».

Выполнение практической работы № 57 «Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

Тема 3.6 Криптозащита информации в сетях передачи данных

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 6. Подготовка реферата на тему: «Криптозащита информации в сетях передачи данных».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 3.7 Защита информации в электронных платежных системах

1. Задание для устного опроса по темам

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

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 58 «Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 7. Подготовка реферата на тему: «Защита информации в электронных платежных системах».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

Тема 3.8. Компьютерная стеганография.

1. Задание для устного опроса по темам

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.

Критерии оценки

«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.

«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 и др.

«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.

«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. Практическая работа

Методические рекомендации по выполнению практических работ.

Выполнение практической работы № 59 «Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ».

Выполнение практической работы № 60 «Реализация простейших стеганографических алгоритмов».

Перечень практических работ и заданий представлен в методических рекомендациях по выполнению практических работ по МДК.02.02 «Криптографические средства защиты информации».

3. Самостоятельная работа

Методические рекомендации по выполнению самостоятельных работ.

СРС № 8. Подготовка доклада-сообщения на тему: «Компьютерная стеганография».

Перечень самостоятельных работ студентов и задания представлены в методических рекомендациях по выполнению самостоятельных работ студентов МДК.02.02 «Криптографические средства защиты информации».

3.2.2. Типовые задания для оценки знаний З1, З2, З3, З4, З5, З6, умений У1, У2, У3, У4, У5, У6, У7, У8, У9, У10 (рубежный контроль)

1. Задание для устного опроса по темам

Контрольная работа № 1 «Криптографические методы защиты информации».

Цель: проверить теоретические знания и практические навыки по темам дисциплины МДК.02.02 «Криптографические средства защиты информации».

Задание. Ответить на поставленные вопросы

Вариант 1

6. Делимость чисел. Признаки делимости. Простые и составные числа. Алгоритм Евклида для нахождения НОД.
7. Методы симметричного шифрования.
8. Основные методы криптоанализа. Криптографические атаки.

Вариант 2

6. Проверка чисел на простоту. Алгоритмы генерации простых чисел.
7. Методы асимметричного шифрования.
8. Кодирование информации. Символьное кодирование. Смысловое кодирование.

Критерии оценки

Отметкой «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.

Отметкой «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.

Отметкой «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.

Отметкой «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 Контрольно-оценочные средства для промежуточной аттестации обучающихся

3.3.1 Контрольно-оценочные средства для промежуточной аттестации обучающихся по учебной дисциплине МДК.02.01 «Программные и программно-аппаратные средства защиты информации».

Предметом оценки являются умения и знания, общие компетенции. Контроль и оценка осуществляются с использованием следующих форм и методов:

Устный опрос.

Практические занятия.

Оценка освоения дисциплины предусматривает проведение экзамена.

I. ПАСПОРТ

Назначение:

КОС предназначен для контроля и оценки результатов освоения учебной дисциплины МДК.02.01 «Программные и программно-аппаратные средства защиты информации» по программе подготовки специалистов среднего звена 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Умения

У1 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У2 - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

У3 - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У4 - применять программные и программно-аппаратные средства для защиты информации в базах данных;

У5 - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У6 - применять математический аппарат для выполнения криптографических преобразований;

У7 - использовать типовые программные криптографические средства, в том числе электронную подпись;

У8 - применять средства гарантированного уничтожения информации;

У9 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У10 - осуществлять 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.

Знания

З1 - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З2 - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З3 - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З4 - основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З5 - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З6 - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

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

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

ОК 03 - Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04 - Работать в коллективе и команде, эффективно взаимодействовать с коллегами,
руководством, клиентами.

ОК 05 - Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06 - Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07 - Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 10 - Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1 - Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2 - Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3 - Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4 - Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5 - Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

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.

II. ВОПРОСЫ ДЛЯ ЭКЗАМЕНА

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.

3.3.2 Контрольно-оценочные средства для промежуточной аттестации обучающихся по учебной дисциплине МДК.02.02 «Криптографические средства защиты информации»

Предметом оценки являются умения и знания, общие компетенции. Контроль и оценка осуществляются с использованием следующих форм и методов:

Устный опрос.

Практические занятия.

Оценка освоения дисциплины предусматривает проведение экзамена.

I. ПАСПОРТ

Назначение:

КОС предназначен для контроля и оценки результатов освоения учебной дисциплины МДК.02.02 «Криптографические средства защиты информации» по программе подготовки специалистов среднего звена 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Умения

У1 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У2 - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

У3 - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

У4 - применять программные и программно-аппаратные средства для защиты информации в базах данных;

У5 - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

У6 - применять математический аппарат для выполнения криптографических преобразований;

У7 - использовать типовые программные криптографические средства, в том числе электронную подпись;

У8 - применять средства гарантированного уничтожения информации;

У9 - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

У10 - осуществлять 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.

Знания

З1 - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

З2 - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;

З3 - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

З4 - основные понятия криптографии и типовых криптографических методов и средств защиты информации;

З5 - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;

З6 - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

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

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

ОК 03 - Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04 - Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05 - Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06 - Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07 - Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 09 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 10 - Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1 - Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2 - Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3 - Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4 - Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5 - Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

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.

II. ВОПРОСЫ ДЛЯ ЭКЗАМЕНА

1. Классификация основных методов криптографической защиты.
2. Методы симметричного шифрования.
3. Шифры замены, пропорциональный шифр.
4. Простая замена, многоалфавитная подстановка.
5. Методы перестановки. Табличная перестановка, маршрутная перестановка.
6. Гаммирование. Гаммирование с конечной и бесконечной гаммами.
7. Основные методы криптоанализа.
8. Криптографические атаки.
9. Криптографическая стойкость. Абсолютно стойкие криптосистемы.
10. Принципы Керкхоффса.
11. Перспективные направления криптоанализа, квантовый криптоанализ.
12. Основные принципы поточного шифрования.
13. Применение генераторов ПСЧ в криптографии.
14. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.
15. Кодирование информации. Символьное кодирование. Смысловое кодирование.
16. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.
17. Компьютеризация шифрования.
18. Аппаратное и программное шифрование.
19. Стандартизация программно-аппаратных криптографических систем и средств.
20. Современные программные и аппаратные криптографические средства.
21. Структурная схема симметричных криптографических систем.

22. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.
23. Симметричные алгоритмы DES, AES.
24. Симметричный алгоритм ГОСТ 28147-89.
25. Симметричный алгоритм RC4.
26. Криптосистемы с открытым ключом. Необратимость систем.
27. Структурная схема шифрования с открытым ключом.
28. Элементы теории чисел в криптографии с открытым ключом.
29. Аутентификация данных. Общие понятия.
30. Электронная цифровая подпись. Основные понятия.
31. Алгоритмы цифровой подписи.
32. MAC.
33. Однонаправленные хеш-функции.
34. Алгоритмы распределения ключей с применением симметричных и асимметричных схем.
35. Протоколы аутентификации.
36. Взаимная аутентификация. Односторонняя аутентификация.
37. Абонентское шифрование. Пакетное шифрование.
38. Защита центра генерации ключей.
39. Криптомаршрутизатор.
40. Пакетный фильтр.
41. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протокола WPA.
42. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протокола WEP.
43. Принципы функционирования электронных платежных систем.
44. Электронные пластиковые карты. Персональный идентификационный номер.
45. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.
46. Скрытая передача информации в компьютерных системах.
47. Проблема аутентификации мультимедийной информации.
48. Защита авторских прав.
49. Методы компьютерной стеганографии.
50. 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.

3.4 Контрольно-оценочные средства для промежуточной аттестации обучающихся по учебной и производственной практике

В период прохождения практики обучающимся ведется дневник практики. Дневник практики обучающегося предполагает собой совершенствование знаний теоретического характера, закрепление и применение их в практической деятельности.

По результатам практики обучающимся составляется отчет, который утверждается организацией.

Защита отчетов организуется в колледже. Обучающийся докладывает результаты выполнения индивидуального задания, отвечает на вопросы руководителя практики.

При определении оценки учитывается:

1) степень и качество отработки обучающимся программы практики и индивидуального задания;

2) содержание и качество оформления отчетных документов.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений, определенные программами практик

3.5 Контрольно-оценочные средства для проведения экзамена (квалификационного)

3.5.1 Общие положения

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

Экзамен включает: практический экзамен, защита портфолио.

Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/ не освоен».

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемых показателям, а также общих компетенций. Условием допуска к экзамену (квалификационному) является положительная аттестация по текущему контролю (защита контрольных работ, тестирование, защита ЛПЗ, решение ситуационных задач) и по промежуточному (МДК.02.01, МДК.02.02, учебной практике УП.02 и производственной практике (по профилю специальности ПП.02)).

3.5.2 Таблица сочетаний, проверяемых ПК и ОК:

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:	**Показатели оценки результата**	**Форма экзамена**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Выполнены установка и настройка отдельных программных, программно-аппаратных средств защиты информации.	Практическое выполнение задания №1
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Обеспечена защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Практическое выполнение задания №1
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Выполнено тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Практическое выполнение задания №1
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	Выполнены обработка, хранение и передача информации ограниченного доступа.	Практическое выполнение задания №1
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Уничтожены информация и носители информации с использованием программных и программно-аппаратных средств.	Практическое выполнение задания №1
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в	Выполнена регистрация основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных	Практическое выполнение задания №1

том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Обоснован выбор метода и средства решения профессиональной задачи. Дана адекватная оценка и самооценка эффективности и качества выполнения профессиональной задачи.	Практическое выполнение задания №2
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Использованы различные источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональной задачи.	Практическое выполнение задания №2
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	Продемонстрирована ответственность за принятые решения. Обоснованы самоанализ и коррекция результатов собственной работы.	Практическое выполнение задания №2
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентам	Продемонстрирована способность работы в коллективе и команде, взаимодействия с коллегами, руководством, клиентами.	Практическое выполнение задания №2
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Продемонстрирована способность осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Практическое выполнение задания №2
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей	Презентовать структуру профессиональной деятельности по профессии (специальности)	Практическое выполнение задания №2
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Соблюдать нормы экологической безопасности. Определять направления ресурсосбережения в рамках профессиональной деятельности по профессии (специальности)	Практическое выполнение задания №2
ОК 08. Использовать средства физической культуры для	Использовать физкультурно-оздоровительную деятельность для	Практическое выполнение

сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	укрепления здоровья, достижения жизненных и профессиональных целей; Применять рациональные приемы двигательных функций в профессиональной деятельности. Пользоваться средствами профилактики перенапряжения характерными для данной профессии (специальности)	задания №2
ОК 09. Использовать информационные технологии в профессиональной деятельности	Эффективно использованы информационно-коммуникационные технологии в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту.	Практическое выполнение задания №2
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	Эффективно использована техническая документация, в том числе на английском языке.	Практическое выполнение задания №2

3.5.3 Результаты **освоения модуля, подлежащие проверке на экзамене (квалификационном) дополнительно**

Общие компетенции, для проверки сформированности которых используется портфолио: ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10.

Требования к портфолио:

Тип портфолио: портфолио смешанного типа,

Основные требования:

Обязательные документы:

- Сводная ведомость оценивания экзамена (квалификационного) по профессиональному модулю **ПМ.02** Защита информации в автоматизированных системах программными и программно-аппаратными средствами;
- аттестационный лист по учебной практике, дневник обучающегося;
- аттестационный лист по производственной практике, дневник обучающегося;
- характеристика профессиональной деятельности обучающегося во время производственной практики;

Дополнительные материалы:

- Доклады участников научно-практических конференций;

- результаты участия во внеурочной научно-исследовательской деятельности;

- Грамоты за спортивные и общественные достижения;

- портфолио в электронном виде (сообщения, рефераты, доклады, отчеты по практическим занятиям, видеоматериалы, фотоматериалы, презентации профессиональной направленности, выполненные обучающимися во время самостоятельной работы);

- свидетельства, подтверждающие участие в коллективных творческих мероприятиях (ведущий тематического вечера, член жюри, участник слета, участник турпохода, и т. д.).

Требования к структуре оформлению и защите портфолио:

1. Портфолио оформляется обучающимся в течение всего периода освоения профессионального модуля, в том числе в период учебной и производственной практики.
2. Оформление в соответствии с эталоном (титульный лист, паспорт портфолио);
3. Защита портфолио в виде компьютерной презентации, выполненной в среде PowerPoint.

Карта формирования общих компетенций

Критерии оценки портфолио

№	Показатель оценки результата	Документ портфолио	Оценка сформированности компетенции (да\нет)
ОК 01.	Выбор и применение способов решения профессиональных задач	дневник (учебной) производственной практики; аттестационные листы	
ОК 02.	Эффективный поиск, анализ и интерпретация информации, необходимой для выполнения задач профессиональной деятельности.	дневник (учебной) производственной практики; аттестационные листы	
ОК 03.	Эффективное планирование и реализация собственного профессионального личностного развития	дневник (учебной) производственной практики; аттестационные листы	
ОК 04.	Выполнение обязанностей в соответствии с ролью в группе; участие в планировании и организации групповой работы	портфолио в электронном виде (сообщения, рефераты, доклады, отчеты по практическим занятиям, видео материалы, фотоматериалы, презентации профессиональной	

		направленности, выполненные обучающимися во время самостоятельной работы)	
ОК 05.	Демонстрация способности осуществления устной и письменной коммуникации на государственном языке с учетом особенностей социального и культурного контекста	портфолио в электронном виде (сообщения, рефераты, доклады, отчеты по практическим занятиям, видео материалы, фотоматериалы, презентации профессиональной направленности, выполненные обучающимися во время самостоятельной работы)	
ОК 06.	Презентация структуры профессиональной деятельности по профессии (специальности)	дневник (учебной) производственной практики; аттестационные листы	
ОК 07.	Соблюдение норм экологической безопасности. Определение направлений ресурсосбережения в рамках профессиональной деятельности по профессии (специальности)	дневник (учебной) производственной практики; аттестационные листы	
ОК 08.	Применение рациональных приемов двигательных функций в профессиональной деятельности. Использование средств профилактики перенапряжения характерных для данной профессии (специальности)	дневник (учебной) производственной практики; аттестационные листы	
ОК 09.	Решение профессиональных задач, связанных с обработкой информации, с использованием информационных технологий	портфолио в электронном виде (сообщения, рефераты, доклады, отчеты по практическим занятиям, видео материалы, фотоматериалы,	

		презентации профессиональной направленности, выполненные обучающимися во время самостоятельной работы)	
ОК 10.	Применение профессиональной документации при решении задач	портфолио в электронном виде (сообщения, рефераты, доклады, отчеты по практическим занятиям, видео материалы, фотоматериалы, презентации профессиональной направленности, выполненные обучающимися во время самостоятельной работы)	

3.6.4 Выполнения задания в ходе экзамена

Комплект экзаменационных материалов

1. Задание для экзаменующегося

Задание 1

Коды проверяемых профессиональных компетенций: **ПК.2.1., ПК. 2.2., ПК.2.3., ПК 2.4., ПК 2.5., ПК 2.6.**

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

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.

Инструкция

Внимательно прочитайте задание.

Время выполнения задания – 40 минут

Текст задания:

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.

ЗАДАНИЕ 2

Коды проверяемых общих компетенций: **ОК 01, ОК 02, ОК 03, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09, ОК 10**

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

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

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания – 40 минут

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.

3.6.5 Пакет экзаменатора

Условия выполнения задания:

Инструкция

Ознакомьтесь с заданиями для экзаменующихся

Количество вариантов заданий (пакетов заданий) для экзаменующихся: 10.

Время выполнения каждого задания и максимальное время на экзамен (квалификационный):

Задание № 1–40 минут

Задание № 2–40 минут

Задание № 3–40 минут

Всего на экзамен – 2 часа

Экзамен проводится в группе в количестве - 19 человек

Методическое обеспечение: Федеральный государственный образовательный стандарт по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, учебный план по профессии, рабочая программа профессионального модуля.

3.6.6 Критерии оценки

Показатель	Результат	Оценка
1. Выполнено задание	+	- не выполнено задание – оценка «неудовлетворительно» - выполнено задание не в полном объеме – оценка «удовлетворительно» - правильно выполнено задание с недочетами – оценка «хорошо» - Правильно выполнено задание – оценка «отлично»
2. Даны ответы на вопросы	+	
3. Проведен анализ программного продукта.	+	
4. Сделаны выводы	+	

Параметры оценивания:

Профессиональные компетенции считаются освоенными при выполнении задания – экзамен «освоен». Если задание не выполнено – экзамен «не освоен».