МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Институт профессионального образования

УТВЕРЖДАЮ:
Проректор-директор ИПО
_____Попов И.П.
«_19_» ____04_____ 2022 г.

Рабочая программа профессиональногомодуля

ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

Специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Присваиваемая квалификация
«Техник по защите информации»

Формы обучения
очная

Кемерово 2022

Рабочую программу составили:

Заведующий кафедры ИБ _____ Е.В. Прокопенко

подпись

Старший преподаватель кафедры ИБ _____ М.О. Пузырев

подпись

Рабочая программа обсуждена на заседании
ЦМК Обеспечение информационной безопасности автоматизированных систем

Протокол № 4 от 04.04 2022

Председатель ЦМК Обеспечение информационной безопасности автоматизированных систем _____ Е.В. Прокопенко

подпись

Согласовано
зам. директора по УР ИПО _____ Н. С. Полуэктова

подпись

Согласовано
зам. директора по МР ИПО _____ Т. Ю. Сьянова

подпись

Оглавление

Рабочую программу составил
Заведующий кафедрой ИБ Е.В. Прокопенко

Рабочая программа обсуждена на заседании
ЦМК Обеспечение информационной безопасности автоматизированных систем
Протокол № 4 от 04.04.2023.

Председатель ЦМК Обеспечение информационной
безопасности автоматизированных систем Е.В. Прокопенко

Согласовано
зам. директора по УР ИПО Н.С. Полуэктова
подпись

Согласовано
зам. директора по МР ИПО Т.Ю. Сьянова

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ.

1.1. Место ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствамив структуре основной образовательной программы

ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами в структуре основной образовательной программы является обязательной частью профессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обеспечивает формирование профессиональных и общих компетенций.

1.2. Цель и планируемые результаты освоения ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

В результате изучения профессионального модуля студент должен освоить вид профессиональной деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами*и соответствующие ему общие и профессиональные компетенции:

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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.

В результате освоения профессионального модуля обучающийся должен:

Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;способы решения задач профессиональной

деятельности, применительно к различным контекстам;номенклатуру информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации;источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;возможные траектории профессионального развития и самообразования;психологию коллектива; психологию личности;современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности;информационно-коммуникационные технологии профессиональной деятельности;правила построения простых и сложных предложений на профессиональные темы;основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации;особенности и способы применения программных средств и гарантированного уничтожения информации; особенности и способы применения аппаратных средств гарантированного уничтожения информации;особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска;использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;выстраивать траектории профессионального и личностного развития;организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение;использовать информационные технологии в профессиональной деятельности;понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты

информации;применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;применять средства гарантированного уничтожения информации;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;

Иметь практический опыт: установки, настройки программных средств защиты информации в автоматизированной системе;обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети;тестирования функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе;

2. СТРУКТУРА И СОДЕРЖАНИЕ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ.

2.1. Объем ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Форма обучения	Количество часов, ОФ				Всего
	5 семестр	6 семестр	7 семестр	8 семестр	
Объем ПМ	**120**	**222**	**270**	**108**	**720**
в том числе:					
Лекции, уроки	50	46	38		134
Лабораторные работы					
Практические занятия	40	54	60		154
Курсовое проектирование			30		30
Консультации	6		10		16
Самостоятельная работа	18	14	24		56
Промежуточная аттестация	6				6
Индивидуальное проектирование					
Учебная практика		108			108
Производственная практика			108	108	216
Промежуточная аттестация (квалификационный экзамен)					

2.2. Тематический план и содержание ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
5 семестр	
МДК 02.02 Криптографические средства защиты информации	**120**
Введение.	
Лекции	
Предмет и задачи криптографии. История криптографии. Основные термины.	1
Самостоятельная работа обучающихся: История развития криптографии	1
Раздел 1. Математические основы защиты информации	
Тема 1.1. Математические основы криптографии	
Лекции	
Лекция 1.1.1. Элементы теории множеств. Группы, кольца, поля.	1
Лекция 1.1.2. Делимость чисел. Признаки делимости. Простые и составные числа.	1
Лекция 1.1.3. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	1
Лекция 1.1.4. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	1
Лекция 1.1.5. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	1
Лекция 1.1.6. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	1
Лекция 1.1.7. Китайская теорема об остатках.	1
Лекция 1.1.8. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	1
Лекция 1.1.9. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	1
Лекция 1.1.10. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	1
Лекция 1.1.11. Арифметические операции над большими числами.	1
Лекция 1.1.12. Эллиптические кривые и их приложения в криптографии.	1
Практические занятия	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практическое занятие 1.1.1. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений.	1
Практическое занятие 1.1.2. Проверка чисел на простоту.	1
Практическое занятие 1.1.3. Решение задач с элементами теории чисел.	1
Самостоятельная работа обучающихся	
1.1.1. Программная реализация классических шифров	2
Раздел 2. Классическая криптография	
Тема 2.1. Методы криптографического защиты информации	
Лекции	
Лекция 2.1. Классификация основных методов криптографической защиты. Методы симметричного шифрования.	1
Лекция 2.1. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.	1
Лекция 2.3. Методы перестановки. Табличная перестановка, маршрутная перестановка. Гаммирование. Гаммирование с конечной и бесконечной гаммами.	1
Практические занятия	
Практическое занятие 2.1.1. Применение классических шифров замены.	1
Практическое занятие 2.1.2. Применение классических шифров перестановки.	1
Практическое занятие 2.1.3. Применение метода гаммирования.	1
Самостоятельная работа обучающихся	
2.1.1. Программная реализация классических шифров	2
Тема 2.2. Криптоанализ	
Лекции	
Лекция 2.2.1. Основные методы криптоанализа. Криптографические атаки.	1
Лекция 2.2.2. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	1
Лекция 2.2.3. Перспективные направления криптоанализа, квантовый криптоанализ.	1
Практические занятия	
Практическое занятие 2.2.1. Криптоанализ шифра простой замены методом анализа	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
частотности символов.	
Практическое занятие 2.2.2. Криптоанализ классических шифров методом полного перебора ключей.	1
Практическое занятие 2.2.3. Криптоанализ шифра Вижинера.	2
Самостоятельная работа обучающихся	
2.2.1. Оптимизация методов частотного анализа моноалфавитных шифров.1	2
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	
Лекции	
Лекция 2.3.1. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.	1
Лекция 2.3.2. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	1
Практические занятия	
Практическое занятие 2.3.1. Применение методов генерации ПСЧ.	2
Раздел 3. Современная криптография	
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	
Лекции	
Лекция 3.1.1. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.	1
Лекция 3.1.2. Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств.	1
Практические занятия	
Практическое занятие 3.1.1. Кодирование информации.	2
Практическое занятие 3.1.2. Программная реализация классических шифров.	2
Практическое занятие 3.1.3. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2
Самостоятельная работа обучающихся	
3.1.1. Методы механизации шифрования	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Тема 3.2. Симметричные системы шифрования	
Лекции	
Лекция 3.2.1. Общие сведения. Структурная схема симметричных криптографических систем.	1
Лекция 3.2.2. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4.	1
Практические занятия	
Практическое занятие 3.2.1. Изучение программной реализации современных симметричных шифров.	2
Самостоятельная работа обучающихся	
3.2.1. Анализ современных симметричных криптоалгоритмов	1
3.2.2. Цифровое представление различных форм информации	1
Тема 3.3. Асимметричные системы шифрования	
Лекции	
Лекция 3.3.1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	1
Лекция 3.3.2. Элементы теории чисел в криптографии с открытым ключом.	1
Практические занятия	
Практическое занятие 3.3.1. Применение различных асимметричных алгоритмов.	2
Практическое занятие 3.3.2. Изучение программной реализации асимметричного алгоритма RSA.	2
Самостоятельная работа обучающихся	
3.3.1. Анализ современных асимметричных криптоалгоритмов	1
Тема 3.4. Аутентификация данных. Электронная подпись	
Лекции	
Лекция 3.4.1. Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	1
Практические занятия	
Практическое занятие 3.4.1. Применение различных функций хеширования, анализ особенностей хешей.	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практическое занятие 3.4.2. Применение криптографических атак на хеш-функции.	2
Практическое занятие 3.4.3. Изучение программно-аппаратных средств, реализующих основные функции ЭП.	2
Самостоятельная работа обучающихся	
3.4.1. Сравнительный анализ функций хеширования	1
3.4.2. Аутентификация сообщений	1
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	
Лекции	
Лекция 3.5.1 Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.	1
Практические занятия	
Практическое занятие 3.5.1. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2
Практическое занятие 3.5.2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2
Тема 3.6. Криптозащита информации в сетях передачи данных	
Лекции	
Лекция 3.6.1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр.	3
Лекция 3.6.2. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов.	4
Тема 3.7. Защита информации в электронных платежных системах	
Лекции	
Лекция 3.7.1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.	4
Лекция 3.7.2. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2
Практические занятия	
Практическое занятие 3.7.1. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей.	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Самостоятельная работа обучающихся	
3.7.1. Законодательство в области криптографической защиты информации	2
Тема 3.8. Компьютерная стеганография	
Лекции	
Лекция 3.8.1. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	4
Лекция 3.8.2. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ.	4
Практические занятия	
Практическое занятие 3.8.1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ.	2
Практическое занятие 3.8.2. Реализация простейших стеганографических алгоритмов.	2
Самостоятельная работа обучающихся	
3.8.1. Программная реализация современных криптоалгоритмов	1
3.8.2. Перспективные направления криптографии	1
Консультации	6
Промежуточная аттестация в форме экзамена	6
МДК 02.02 Криптографические средства защиты информации	**120**
6 семестр	
МДК.02.01 Программные и программно-аппаратные средства защиты информации	**114**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации	
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	
Лекции	
Лекция 1.1.1 Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации.Классификация методов и средств программно-аппаратной защиты информации	1
Тема 1.2. Стандарты безопасности	
Лекции	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 1.2.1. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2
Лекция 1.2.2. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
Практические занятия	
Практическое занятие 1.2.1. 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.	4
Практическое занятие 1.2.2. Обзор стандартов. Работа с содержанием стандартов	4
Тема 1.3. Защищенная автоматизированная система	
Лекции	
Лекция 1.3.1. Автоматизация процесса обработки информации, Понятие автоматизированной системы. , Особенности автоматизированных систем в защищенном исполнении., Основные виды АС в защищенном исполнении., Методы создания безопасных систем, Методология проектирования гарантированно защищенных КС, Дискреционные модели, Мандатные модели	1
Практические занятия	
Практическое занятие 1.3.1. Учет, обработка, хранение и передача информации в АИС, Ограничение доступа на вход в систему, Идентификация и аутентификация пользователей, Разграничение доступа.	4
Практическое занятие 1.3.2. Регистрация событий (аудит)., Контроль целостности данных, Уничтожение остаточной информации.	2
Практическое занятие 1.3.3. Управление политикой безопасности. Шаблоны безопасности, Криптографическая защита. Обзор программ шифрования данных, Управление политикой безопасности. Шаблоны безопасности	2
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	
Лекции	
Лекция 1.4.1. Источники дестабилизирующего воздействия на объекты защиты. Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практические занятия	
Практическое занятие 1.4.1.Распределение каналов в соответствии с источниками воздействия на информацию	2
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	
Лекции	
Лекция 1.5.1. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД	1
Лекция 1.5.2. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам. Доступ к данным со стороны процесса	1
Лекция 1.5.3. Особенности защиты данных от изменения. Шифрование.	1
Практические занятия	
Практическое занятие 1.5.1. Организация доступа к файлам	2
Практическое занятие 1.5.2. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2
Самостоятельная работа. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.	8
Раздел 2. Защита автономных автоматизированных систем	
Тема 2.1. Основы защиты автономных автоматизированных систем	
Лекции	
Лекция 2.1.1. Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	1
Тема 2.2.Защита программ от изучения	
Лекции	
Лекция 2.2.1. Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение. Задачи защиты от изучения и способы их решения. Защита от отладки. Защита от дизассемблирования. Защита от трассировки по	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
прерываниям.	
Тема 2.3. Вредоносное программное обеспечение	
Лекции	
Лекция 2.3.1 Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.Бот-неты. Принцип функционирования. Методы обнаружения. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме". Основные концепции построения систем антивирусной защиты на предприятии.	2
Практические занятия	
Практическое занятие 2.3.1. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
Тема 2.4. Защита программ и данных от несанкционированного копирования	
Лекции	
Лекция 2.4.1. Несанкционированное копирование программ как тип НСД.Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПОк аппаратному окружению и носителям.Защитные механизмы в современном программном обеспечении на примере MS Office.	1
Практические занятия	
Практическое занятие 2.4.1. Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	2
Тема 2.5. Защита информации на машинных носителях	
Лекции	
Лекция 2.5.1. Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов. Безвозвратное удаление данных. Принципы и алгоритмы.	1
Практические занятия	
Практическое занятие 2.5.1. Применение средства восстановления остаточной информации на примере Foremost или аналога	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практическое занятие 2.5.2. Применение специализированного программно средства для восстановления удаленных файлов	2
Практическое занятие 2.5.3. Применение программ для безвозвратного удаления данных	2
Практическое занятие 2.5.4. Применение программ для шифрования данных на съемных носителях	2
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	
Лекции	
Лекция 2.6.1. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ. Устройства TouchMemory.	1
Тема 2.7. Системы обнаружения атак и вторжений	
Лекции	
Лекция 2.7.1. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ.Программный компонент СОВ.Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	1
Практические занятия	
Практическое занятие 2.7.1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2
Самостоятельная работа. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.	6
Раздел 3. Защита информации в локальных сетях	
Тема 3.1. Основы построения защищенных сетей	
Лекции	
Лекция 3.1.1. Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	8
Тема 3.2. Средства организации VPN	
Лекции	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 3.2.1. Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.	10
Практические занятия	
Практическое занятие 3.2.1 Развертывание VPN	10
Раздел 4. Защита информации в сетях общего доступа	
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	
Лекции	
Лекция 4.1.1. Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня. Однохостовые и мультихостовыеfirewall. Основные типы архитектур мультихостовыхfirewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов.	10
Практические занятия	
Практическое занятие 4.1.1. Изучение и сравнение архитектур DualHomedHost, BastionHost, Perimetr. Изучение различных способов закрытия "опасных" портов	8
7 семестр	**162**
Раздел 5. Защита информации в базах данных	
Тема 5.1. Защита информации в базах данных	
Лекции	
Лекция 5.1.1. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	10
Практические занятия	
Практическое занятие 5.1.1. Изучение механизмов защиты СУБД MS Access. Изучение штатных средств защиты СУБД MSSQL Server	12
Самостоятельная работа	10
Раздел 6. Мониторинг систем защиты	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Тема 6.1. Мониторинг систем защиты	
Лекции	
Лекция 6.1.1. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2
Лекция 6.1.2. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	2
Лекция 6.1.3. Классификация отслеживаемых событий. Особенности построения систем мониторинга	4
Лекция 6.1.4. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	2
Лекция 6.1.5. Классификация сетевых мониторов.	2
Лекция 6.1.6. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	2
Практические занятия	
Практическое занятие 6.1.1. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов.	10
Практическое занятие 6.1.2. Проведение аудита ЛВС сетевым сканером	10
Тема 6.2. Изучение мер защиты информации в информационных системах	
Лекции	
Лекция 6.2.1. Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	4
Практические занятия	
Практическое занятие 6.2.1. Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	28
Тема 6.3. Изучение современных программно-аппаратных комплексов.	
Лекции	
Лекция 6.3.1. Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других	10

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах
аналогов. Изучение типовых решений для построения VPN на примере VipNet или других аналогов. Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов		
Самостоятельная работа		14
Консультации		10
Курсовая работа (проект), в том числе:		30
Курсовая работа (проект) - выполнение		28
Промежуточная аттестация в форме защиты курсовой работы(проекта)		2
МДК.02.01 Программные и программно-аппаратные средства защиты информации		**276**
Учебная практика УП 02.01		**216**
Вид профессиональной деятельности: Защита информации в автоматизированных системах программными и программноаппаратными средствами		
Программные и программно-аппаратные средства защиты информации.	Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.	20
	Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности.	20
	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.	20
	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.	22
	Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации.	20
	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	20

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах
	Устранение замечаний по результатам проверки.	20
	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	24
Криптографические средства защиты информации.	Применение математических методов для оценки качества и выбора наилучшего программного средства.	24
	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.	26
Всего по УП 02.01.		**216**
8 семестр		
Производственная практика ПП 02.01		**108**
Вид профессиональной деятельности: Защита информации в автоматизированных системах программными и программноаппаратными средствами		
	Консультация	2
Программные и программноаппаратные средства защиты информации. Криптографические средства защиты информации.	Анализ принципов построения систем информационной защиты производственных подразделений.	16
	Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.	16
	Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;	16
	Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении	18
	Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации	20

	Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	20
Всего по ПП 02.01:		**108**
Всего по ПМ 02		**720**

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ.

3.1. Специальные помещения для реализации программы

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:
Комплект мебели (столы и стулья). Проектор. Персональный компьютер.
Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:
Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.
Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3. Специальное помещение № 1251 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:
Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.
Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

4. Специальное помещение № 1139 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:
Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.
Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

5. Специальное помещение № 1147 представляет собой помещение для групповых и

индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь

Помещение для самостоятельной работы обучающихся:

6. Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Помещение для самостоятельной работы обучающихся:

7. Специальное помещение № 1211 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

8. Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:

Перечень основного оборудования:

Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры

Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,

СПРУТ-ОКП

9. Специальное помещение №1251 представляет собой лабораторию программных и программно-аппаратных средств защиты информации, оснащенную антивирусными программными комплексами; программно-аппаратными средствами защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности; программными и программно-аппаратными средствами обнаружения вторжений; средствами уничтожения остаточной информации в запоминающих устройствах;

программными средствами выявления уязвимостей в автоматизированных системам и средствах вычислительной техники; программными средствами криптографической защиты информации; программными средствами защиты среды виртуализации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2. Информационное обеспечение реализации программы

3.2.1. Основная литература

1. Батаев, А. В. Операционные системы н среды: учебник для образовательных учреждении среднего профессионального образования по укрупненной группе специальностей "Информатика и вычислительная техника' / А. В. Батаев. II. Ю. Малютин, С. В. Синнцын ; А. В. Батаев. И. Ю. Малютин, С. В. Снницын. - 5-е издание переработанное - Москва : Академия. 2021. - 285 с. с. - (Мрофессиональное образование :Информатика и вычислительная техника). - URL: https://academiamoscow.ru/reader/?id=539321(дата обращения: 06.05.2022). - Текст : электронный.

3.2.2. Дополнительная литература

1. Рудаков. А. В. Операционные системы и среды: Учебник для СПО / А. В. Рудаков. - Москва: НИЦ ИНФРА-М. 2021. - 304 с. - ISBN 978-5-906923-85-1. - URL: http://znanium.com/catalog/document?id=376576(дата обращения: 06.05.2022). -Текст: электронный.

3.2.3. Методическая литература

1. Профессиональный цикл: методические материалы для обучающихся направления подготовки10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасскийгосударственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности,составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово: КузГТУ, 2020. – 290 с. – URL:http://library.kuzstu.ru/meto.php?n=9964 (дата обращения: 28.02.2023). – Текст: электронный.

2. Методические указания по оформлению отчетов по практике, курсовых работ (проектов) и выпускных квалификационных работ: для всех специальностей СПО / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информатики и информационных систем, составители: Н. С. Полуэктова, Т. С. Семенова. – Кемерово: КузГТУ, 2022. – 1 файл (762 Кб). – URL:http://library.kuzstu.ru/meto.php?n=10478(дата обращения: 28.02.2023). – Текст: электронный.

3.2.4. Интернет-ресурсы

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.
3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.
4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.
5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.
6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.
7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
8. Гарант.ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.
9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.
10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.
11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля). Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

5.1. Паспорт фонда оценочных средств

Планируемые результаты обучения по модулю.
Модуль направлен на формирование следующих компетенций выпускника:

МДК 02.01 Программные и программно-аппаратные средства защиты информации					
№	Наименование разделов дисциплины	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
	Раздел 1. Основные принципы программной и программно-аппаратной защиты информации	Тема 1.1. Предмет и задачи программно-аппаратной защиты информации Тема 1.2. Стандарты безопасности Тема 1.3. Защищенная автоматизированная система Тема 1.4. Дестабилизирующее воздействие на объекты защиты Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	ОК 01.	**Знать**: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; **Уметь:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
			ОК 02.	**Знать:** номенклатуру информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; **Уметь:** определять задачи поиска информации; определять необходимые	

				источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска;	
			ОК 03.	**Знать:** возможные траектории профессионального развития и самообразования; **Уметь:** выстраивать траектории профессионального и личностного развития;	
			ОК 04.	**Знать:** психологию коллектива; психологию личности; **Уметь:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;	
			ОК 09.	**Знать:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности. **Уметь: п**рименять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение	
			ОК 10.	**Знать:** правила построения простых и сложных предложений на	

				профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; **Уметь:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы;	
			ПК 2.1.	**Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **Уметь:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	

				Иметь практический опыт: установки, настройки программных средств защиты информации в автоматизированной системе;	
			ПК 2.4.	**Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **Уметь:** применять программные и программно-аппаратные средства для защиты информации в базах данных; **Иметь практический опыт:** решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;	
	Раздел 2. Защита автономных автоматизированных систем	Тема 2.1. Основы защиты автономных автоматизированных систем Тема 2.2.Защита программ от изучения Тема 2.3. Вредоносное программное обеспечение Тема 2.4. Защита программ и данных от несанкционированного копирования	ПК 2.2.	**Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации в операционных системах; **Уметь:** устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; **Иметь практический опыт:** обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование

		Тема 2.5. Защита информации на машинных носителях Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей Тема 2.7. Системы обнаружения атак и вторжений	ПК 2.3.	**Знать:** методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; **Уметь:** диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; **Иметь практический опыт:**тестирования функций, диагностики, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;	
			ПК 2.4	**Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных; **Уметь:** проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; **Иметь практический опыт:** применения электронной подписи;	
	Раздел 3. Защита информации в локальных сетях	Тема 3.1. Основы построения защищенных сетей Тема 3.2. Средства	ПК 2.5.	**Знать:** особенности и способы применения программных средств и гарантированного уничтожения информации;	опрос обучающихся по контрольным вопросам, защита отчетов по

		организации VPN		**Уметь:** применять средства гарантированного уничтожения информации; **Иметь практический опыт:** учёта, обработки, информации, для которой установлен режим конфиденциальности;	лабораторным заданиям, тестирование, выполнение и защита курсовой работы (проекта)
	Раздел 4. Защита информации в сетях общего доступа	Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	ПК 2.4.	**Знать**: типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; **Уметь:** применять математический аппарат для выполнения криптографических преобразований; **Иметь практический опыт:** применения симметричных и асимметричных криптографических алгоритмов;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование, выполнение и защита курсовой работы (проекта)
			ПК 2.5.	**Знать:** особенности и способы применения аппаратных средств гарантированного уничтожения информации; **Уметь:** выбирать средства гарантированного уничтожения информации; **Иметь практический опыт:** хранения и передачи информации, для которой установлен режим конфиденциальности;	
	Раздел 5. Защита информации в базах данных	Тема 5.1. Защита информации в базах данных	ПК 2.2.	**Знать:** особенности и способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях,	опрос обучающихся по контрольным вопросам, защита отчетов по

				базах данных; **Уметь:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Иметь практический опыт:** использования программных и программно-аппаратных средств для защиты информации в сети;	лабораторным заданиям, тестирование, выполнение и защита курсовой работы (проекта)
			ПК 2.4.	**Знать:** основные понятия криптографии и типовых криптографических методов и средств защиты информации; **Уметь:** использовать типовые программные криптографические средства, в том числе электронную подпись; **Иметь практический опыт:** использования средств шифрования данных;	
	Раздел 6. Мониторинг систем защиты	Тема 6.1. Мониторинг систем защиты Тема 6.2. Изучение мер защиты информации в информационных системах Тема 6.3. Изучение современных программно-аппаратных комплексов.	ПК 2.6.	**Знать:** типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; **Уметь:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование

				средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; **Иметь практический опыт:** работы с подсистемами регистрации событий; выявления событий и инцидентов безопасности в автоматизированной системе;	
МДК 02.02 Криптографические средства защиты информации					
№	**Наименование разделов дисциплины**	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
1	**Введение. Предмет и задачи криптографии. История криптографии. Основные термины.**	Предмет и задачи криптографии. История криптографии. Основные термины.	ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	опрос обучающихся по контрольным вопросам, тестирование,
2	**Раздел 1. Математические**	Тема 1.1. Математические	ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов	опрос обучающихся по контрольным

	основы защиты информации	основы криптографии		и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	вопросам, защита отчетов по практическим заданиям, тестирование
3	**Раздел 2. Классическая криптография**	Тема 2.1. Методы криптографического защиты информации Тема 2.2. Криптоанализ Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
			ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации;	

				Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	
4	**Раздел 3. Современная криптография**	Тема 3.1. Кодирование информации. Компьютеризация шифрования. Тема 3.2. Симметричные системы шифрования Тема 3.3. Асимметричные системы шифрования Тема 3.4. Аутентификация данных. Электронная подпись Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации Тема 3.6. Криптозащита информации в сетях	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись;	

		передачи данных Тема 3.7. Защита информации в электронных платежных системах Тема 3.8. Компьютерная стеганография		Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	
УП 02.01 Учебная практика					
Вид профессиональной деятельности		**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**	
Защита информации в автоматизированных системах программными и программноаппаратными средствами		ПК 2.4	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; **Умения:** применять программные и программно-аппаратные средства для защиты	Проверка отчёта по разделам практики.	

		информации в базах данных;проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; **Практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;применение электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных	
ПП 02.01 Производственная практика			

Вид профессиональной деятельности	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
Защита информации в автоматизированных системах программными и программноаппаратными средствами	ПК 2.1	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Практический опыт:** установка, настройка программных средств защиты информации в автоматизированной системе;	Проверка отчёта по разделам практики.
	ПК 2.2	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; **Умения:** устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Практический опыт:** обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты	Проверка отчёта по разделам практики.

		информации в сети;	
	ПК 2.3	**Знания:** методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; **Умения:** диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; **Практический опыт:** тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации;	Проверка отчёта по разделам практики.
	ПК 2.4	**Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации; **Умения:** применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения	Проверка отчёта по разделам практики.

		криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; **Практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;	
	ПК 2.5	**Знания:** особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; **Умения:** применять средства гарантированного уничтожения информации; **Практический опыт:** учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности;	Проверка отчёта по разделам практики.
	ПК 2.6	**Знания:** типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов	Проверка отчёта по разделам практики.

		информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; **Практический опыт:** работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе;	

5.2. Типовые контрольные задания или иные материалы

5.2.1. Оценочные средства при текущем контроле

5.2.1.1. МДК.02.01. Программные и программно-аппаратные средства защиты информации

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Как реализуется мониторинг систем защиты сети?
2. Как реализуется мониторинг систем защиты серверов?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Основные принципы программной и программно-аппаратной защиты информации

Тема 1.1. Предмет и задачи программно-аппаратной защиты информации

1. В чем состоят основные задачи программно-аппаратной защиты информации?
2. Что является предметом рассмотрения и внимания при создании программно-аппаратных методов и средств защиты информации?
3. Чем характерны задачи программно-аппаратной защиты информации?
4. Знаний в каких предметных областях требует программно-аппаратная защиты информации?
5. Что является предметом исследования и изучения при проектировании средств программно-аппаратных средств защиты информации?
6. Основные понятия программно-аппаратной защиты информации
7. По каким критериям можно классифицировать метод и средства программно-аппаратной защиты информации?
8. Кто осуществляет контроль выполнения задач, связанных с программно-аппаратной защитой информации на конкретном предприятии?
9. Кто является постановщиком задач, связанных с программно-аппаратной защитой информации на конкретном предприятии?
10. Кто несет ответственность за выполнение задач, связанных с программно-аппаратной защитой информации на конкретном предприятии?

Тема 1.2. Стандарты безопасности

1. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
2. Для кого проявляются преимущества от введения стандартов в области ИБ?
3. Какие важнейшие функции выполняют стандарты в области информационной безопасности?
4. Что является основными областями стандартизации информационной безопасности?

5. Какой стандарт является одним из наиболее известных стандартов, источником лучших практик при построении систем управления информационной безопасностью?

6. Какие государственные структуры разрабатывают стандарты по ИБ?

7. Какие государственные структуры имеют право контролировать соблюдение стандартов по ИБ?

8. Какие международные стандарты используются в сфере ИБ в российских предприятиях и учреждениях?

9. Приведите примеры учреждений / предприятий, в которых соблюдение стандартов ИБ является обязательным

10. Каким образом лучшие уникальные практики или решения могут впоследствии стать стандартов в области ИБ?

Тема 1.3. Защищенная автоматизированная система

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

2. Какой протоколов относится к протоколам защищенной передачи данных в сети Интернет?

3. На основе чего программные средства обеспечивают состояние защищенности ИС?

4. Как называется характеристика, определяющая степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования?

5. Сколько классов защищенности автоматизированных систем от несанкционированного доступа существует по документам контролирующих органов?

6. Какие требования предъявляются к технологии учета и хранения информации в защищенных АИС?

7. Какие требования предъявляются к режимам обработки информации на компьютере в защищенных АИС?

8. Какие требования предъявляются к созданию учётных записей пользователей в защищенных АИС?

9. Какие требования предъявляются к механизмам разграничения доступа в защищенных АИС?

10. Какие требования предъявляются к технологиям передачи и представления информации в защищенных АИС?

Тема 1.4. Дестабилизирующее воздействие на объекты защиты

1. Кто или что может являться источником дестабилизирующего воздействия на информацию?

2. По каким критериям классифицируются виды и способы дестабилизирующего воздействия на защищаемую информацию?

3. Какие виды дестабилизирующего воздействия, приводящие к уничтожению, искажению и блокированию информации возможны со стороны людей?

4. Какие условия можно отнести к создающим возможность для дестабилизирующего воздействия на информацию?

5. Какие причины могут оказать дестабилизирующее воздействие на информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи?

6. Какими свойствами должен обладать объект защиты, чтобы минимизировать вероятность дестабилизирующего воздействие на него?

7. Какие последствия могут отразиться на объекте защиты в результате дестабилизирующего воздействия на него со стороны человека?

8. Какие последствия могут отразиться на объекте защиты в результате дестабилизирующего воздействия техногенного характера на него?

9. Какими свойствами должна обладать АИС, чтобы быть максимально устойчивой к дестабилизирующим воздействиям на него?

10. Как и с учетом чего производится оценка вероятности дестабилизирующего воздействия на объект защиты при проектировании АИС?

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

1. Какие существуют основные группы программно-аппаратных средства защиты информации?
2. Приведите примеры средств защиты от НСД в информационных сетях?
3. В чем заключается принцип работы программно-аппаратной системы КРИПТОН ?
4. Какие задачи решает система криптографической защиты информации (СКЗИ) «Верба-0»?
5. Какие основные функции выполняются программно-аппаратными средствами защиты от НСД?
6. Как регистрация событий (аудит) помогает противостоять НСД?
7. Как разграничение доступа помогает противостоять НСД?
8. Как идентификация и аутентификация пользователей помогает противостоять НСД?
9. Каким принципам должна удовлетворять АИС, чтобы эффективно противостоять НСД?
10. По каким методикам и критериям оценивается возможность АИС противостоять НСД??

Раздел 2. Защита автономных автоматизированных систем

Тема 2.1. Основы защиты автономных автоматизированных систем

1. Что необходимо обеспечить при использовании Flash-Bios в автоматизированных рабочих местах на базе автономных ПЭВМ?
2. Какое средство защиты позволяет выявлять несанкционированный доступ (или попытки несанкционированного доступа) к ресурсам автономной автоматизированной системы?
3. Какими качествами должна обладать автономная автоматизированная система?
4. Перечислите основные аспекты защиты автономных систем
5. Приведите примеры программно-аппаратных средств защиты, которые могут использоваться для автономных автоматизированных систем
6. Перечислите основные категории мероприятий, способствующие обеспечению защиты АС
7. Что является наиболее важным объектом защиты в ИС?
8. В чем преимущества и недостатки автономных автоматизированных систем с точки зрения их защиты?
9. По каким методикам и критериям оценивается степень защиты автономных автоматизированных систем?
10. Способствует ли усилению защиты автономных автоматизированных систем использование нестандартного ПО?

Тема 2.2.Защита программ от изучения

1. Какие методы используют для защиты программ от изучения?
2. По отношению к каким процессам должна быть устойчива защищенная программа?
3. Какие существуют наиболее известные способы защиты программы от получения кода программы на языке низкого уровня?
4. Какие существуют наиболее известные способы защиты программы от работы под контролем отладчика?
5. Какие компоненты должна включать защищаемая от исследования программа?
6. В чем состоят отрицательные моменты защиты программ от изучения?
7. Как оценивается адекватность уровня защиты от изучения для конкретной программы?
8. Категории каких программ необходимо защищать от изучения?
9. Имеются ли какие-то стандарты на защиту программ от изучения?
10. Как происходит выбор методов и средств защиты программ от изучения?

Тема 2.3. Вредоносное программное обеспечение

1. Какие типы программ являются вредоносными?

2. Что является критерием вредоносности программ?
3. Что такое сетевые черви?
4. Как называется тип вредоносной программы, которая подменяет собой загрузку некоторых программ при старте системы?
5. Какой тип вируса поражает документы?
6. Какие типы вирусов опасны только при работе в сети?
7. Что такое и как работает программа-шифровальщик?
8. Что такое и как работает фишинговая программа?
9. Что такое и как работает программа-вымогатель?
10. Что такое и как работает программа-шпион?

Тема 2.4. Защита программ и данных от несанкционированного копирования

1. Какие основные меры защиты от НСК существуют?
2. В каком виде реализуется защита программ, установленных на жёстком диске?
3. В чем состоят основные мотивы создания и использования систем защиты от копирования?
4. Перечислите некоторые основные требования, предъявляемые к системе защиты от копирования?
5. В каком виде реализуется защита от копирования файлов, находящихся на съемных носителях?
6. Приведите примеры программных средств защиты от копирования
7. приведите примеры аппаратных средств защиты от копирования
8. Какие критерии используются для оценки эффективности защиты от копирования?
9. На основе чего производится выбор средств защиты от копирования?
10. Какие программы или данные требуют защиты от копирования?

Тема 2.5. Защита информации на машинных носителях

1. Из каких мероприятий состоит процедура защиты машинных носителей информации (ЗНИ)?
2. Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации?
3. Если в АС работает один пользователь, который допущен ко всей информации и эта информация размещена на носителях одного уровня конфиденциальности, то к какой группе относится такая АС ?
4. Какая информация может использоваться при учете машинных носителей информации?
5. Какое из программных средств позволяет выполнять поиск остаточной информации на машинных носителях, а также учет носителей?
6. Что обычно оговаривается в большинстве типовых инструкций по защите машинных носителей информации?
7. На какие типы подразделяются машинные носители информации?
8. Какие носители информации более подвержены техногенным деструктивным воздействиям по отношению к хранимой информации?
9. Какие носители информации более подвержены деструктивным воздействиям, вызванным человеком по отношению к хранимой информации?
10. Приведите пример нормативного документа по защите информации на машинных носителях в типовом офисе госучреждения

Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей

1. Как называется устройство (тип устройства) для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающее маленький пейджер, не присоединяемый к компьютеру и имеющий собственный источник питания?
2. Какие бывают виды смарт-карт по техническому исполнению?
3. Какие устройства могут различаться между собой физически, но выполнять одну и ту же функцию и иметь подобный принцип действия?

4. Какое из устройств чаще всего имеет форму флэш-памяти?
5. Какие системы биометрической идентификации являются наименее затратными?
6. Каким образом можно усилить степень защиты во время аутентификации пользователей при использовании токенов или смарт-карт?
7. Какое из известных вам устройств аутентификации является наиболее надежным?
8. В чем отличие Рутокена от Е-токена ?
9. Какая особенность работы со смарт-картами является одновременно недостатком и дополнительным элементом защиты?
10. В чем недостатки биометрических систем идентификации, работающих на основе сканирования формы и размера лица, голоса?

Тема 2.7. Системы обнаружения атак и вторжений

1. По каким параметрам может группироваться информация, полученная об информационной атаке анализирующим сервером?
2. Для чего используются протокольные системы обнаружения вторжений?
3. Что включает в себя архитектура системы обнаружения вторжений?
4. Подключаясь к чему сетевая система обнаружения вторжений получает доступ к сетевому трафику?
5. Каких видов существуют системы обнаружения вторжений?
6. Каким образом можно моделировать проведения атаки?
7. Какие существуют методы обнаружения вторжений?
8. Приведите пример активных и пассивных систем обнаружения вторжений
9. Какие существуют стандарты в области систем обнаружения вторжений?
10. Как оценивается эффективность систем обнаружения атак и вторжений?

Раздел 3. Защита информации в локальных сетях

Тема 3.1. Основы построения защищенных сетей

1. Что представляет собой контроль защищенности информационной сети?
2. В какой политике безопасности для доступа к любому защищаемому объекту сети применяется запретительное правило: все, что не разрешено явно – запрещено?
3. Каково основное назначение межсетевого экрана в защищенной информационной сети?
4. Приведите пример системы анализа защищенности сети?
5. На каком этапе работают механизмы защиты, реализованные в межсетевых экранах, серверах аутентификации, системах разграничения доступа?
6. Какие виды защиты должны иметь сервера корпоративной сети?
7. Какие виды защиты должны иметь рабочие станции корпоративной сети?
8. Каким требованиям должна удовлетворять кабельная система защищенных сетей?
9. Какие протоколы должны использоваться при обращении к корпоративному веб-серверу в защищенных сетях?
10. Приведите примеры стандартов на проектирование корпоративной защищенной сети

Тема 3.2. Средства организации VPN

1. При логическом группировании в виртуальных ЛКС какие используются процедуры управления пакетами?
2. На каком уровне модели OSI строятся наиболее распространенные VPN-системы?
3. Какая топология реализуется в виртуальной частной сети?
4. С какой целью часто используются VPN типа «маршрутизатор—маршрутизатор»?
5. На основе чего строятся аппаратные сети VPN?
6. В чем основной принцип действия и создания VPN?
7. Какие протоколы используются в работе VPN?
8. В чем преимущества и недостатки облачных VPN-сервисов?
9. Приведите пример облачных сервисов, с помощью которых можно очень быстро создать подобие VPN, например, для задач удалённого доступа.
10. На базе каких ОС можно организовать VPN-сервер предприятия?

Раздел 4. Защита информации в сетях общего доступа

Тема 4.1.Обеспечение безопасности межсетевого взаимодействия

1. 1.Что такое межсетевое экранирование? Какие функции оно выполняет?
2. Что является самым главным в настройках межсетевого экрана (брандмауэра)?
3. Перечислите основные положения политики сетевой безопасности.
4. Какие бывают типы межсетевых экранов?
5. Какие требования предъявляются к межсетевым экранам?
6. Перечислите типы межсетевых экранов и их основные характеристики.
7. Сформулируйте понятие «брандмауэр».
8. Что фиксирует журнал безопасности брандмауэра?
9. Какой протокол обеспечения сетевой безопасности является частью протокола IPSec и выполняет функции обеспечения целостности данных, защиты от повторения данных, удостоверения источника данных?
10. Какой компонент защиты как минимум должен присутствовать в локальных и корпоративных сетях для обеспечения информационной безопасности?

Раздел 5. Защита информации в базах данных

Тема 5.1. Защита информации в базах данных

1. Созданная каким методом копия базы данных позволяет восстановить информацию полностью на 100% при сбое в любой момент времени?
2. Что является самым надежным способом защиты данных от потери в БД?
3. Можно ли модель полного восстановления использовать для рабочей БД, содержащей критически важные данные?
4. Может ли простая модель восстановления использоваться при разработке БД или при работе с базами, которые не требуют частого редактирования?
5. В чем основные направления защиты в базах данных?
6. Как реализуется физическая и логическая целостность базы данных на примере MS Access?
7. Какие бывают типы разрешений на доступ к базе данных на примере MS Access?
8. Как реализуется защита базы данных на уровне пароля, на уровне пользователя на примере MS Access?
9. Каким образом должна быть обеспечена сетевая защита сервера БД?
10. Какие существуют стандарты на качество защиты БД?

Раздел 6. Мониторинг систем защиты

Тема 6.1. Мониторинг систем защиты

1. В каких направлениях можно развивать систему мониторинга действий по защите конфиденциальной информации?
2. Является ли построение системы предотвращения утечек дальнейшим развитием системы мониторинга действий по защите конфиденциальной информации?
3. Какое аппаратное обеспечение информационной системы подлежит защите и мониторингу?
4. Какой механизм подотчётности пользователей позволяет выполнять мониторинг нарушений целостности информации?
5. Что может включать в себя мониторинг систем защиты информации?
6. Как реализуется мониторинг систем защиты помещений?
7. Как реализуется мониторинг систем защиты сети?
8. Как реализуется мониторинг систем защиты серверов?
9. Как реализуется мониторинг систем защиты рабочих станций?
10. Как и кем осуществляется аудит средств мониторинга систем защиты?

Тема 6.2. Изучение мер защиты информации в информационных системах

1. Относится ли планирование бесперебойной работы организации к ключевым индикаторам в методиках оценки принимаемых мер по обеспечению информационной безопасности?

2. На чем основывается подход к анализу и оценке принимаемых мер по обеспечению информационной безопасности?
3. Какая методика является самой важной при выборе конкретных защитных мер?
4. За счет каких типов мер обеспечивается информационная безопасность?
5. Что следует учитывать при анализе стоимости защитных мер?
6. В чем состоит внешняя безопасность ИС?
7. В чем состоит внутренняя безопасность ИС?
8. Сформулируйте основные принципы построения систем защиты ИС
9. Кто и на основании чего оценивает адекватность выбранных мер защиты ИС?
10. Что относится к процедурным мерам защиты ИС?

Тема 6.3. Изучение современных программно-аппаратных комплексов.

1. Как называется абстрактное описание комплекса программно-технических средств и организационных мер защиты от несанкционированного доступа к информации?
2. Перечислите типовые методы изучения современных программно-аппаратных комплексов в условиях учебного заведения
3. Перечислите типовые методы изучения современных программно-аппаратных комплексов в реальных рабочих условиях
4. При каком методе изучения достигается наилучший эффект при изучении программно-аппаратного комплекса?
5. На кого возлагается ответственность за исправность и правильную работу программно-аппаратного комплекса после изучения?
6. С точки зрения программно-аппаратного комплекса SecretNetStudio из скольких уровней состоит комплексная защита ИС?
7. Перечислите основные назначения и возможности приложения MaxPatrol
8. Перечислите основные назначения и возможности приложения InfoWatch Traffic Monitor
9. Что такое DLP системы?
10. Приведите примеры программно-аппаратных анализаторов сетевых протоколов

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1. Тема работы.
2. Задачи задания.
3. Краткое описание хода выполнения.
4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).
5. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. В чем состоит внешняя безопасность ИС?
2. В чем состоит внутренняя безопасность ИС?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1. Задание к практическому занятию 1.2.1. 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.

Задание 1. Определить нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 2. Изучить ФЗ «Об информации, информационных технологиях и о защите информации». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 3. Изучить приказ ФСТЭК России от 18 февраля 2013 г.; 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 4. Изучить типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством Центра ФСБ России 21.02.2008 №149/6/6-622. Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.2.2. Обзор стандартов. Работа с содержанием стандартов

Задание 1. Выписать государственные стандарты в области информационной безопасности.

Задание 2. Выписать международные стандарты информационной безопасности.

Задание 3. Изучить ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 1.3.1. Учет, обработка, хранение и передача информации в АИС, Ограничение доступа на вход в систему., Идентификация и аутентификация пользователей, Разграничение доступа.

Задание 1. Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. 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?

Задание 2. Изучить технологический процесс обработки информации. Перечислить и охарактеризовать технологические процессы процесса обработки информации. В чем заключается

различие между централизованным и децентрализованным способами обработки информации? Какие режимы обработки информации вам известны?

Задание 3. Изучить технологии передачи и представления информации. Описать, как происходит передача данных.

Задание 4. Продумать и создать технологию учета и отработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудования «Сервис-ТЕХНО». Результат выполнения задания оформить в виде таблицы.

Задание 5. Используя технологии поиска информации, найдите разницу между терминами “хранение” и “сохранение данных”.

Задание 6. Используя средства Интернета, перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

Задание 7. Ознакомиться с технологиями создания и управления учетными записями пользователей в ОС Windows.

Задание 8. Создайте новую учетную запись пользователя с помощью командной строки.

Задание 9. 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.

Задание 10. 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.

Задание 11. Опишите параметры локальной политики безопасности операционной системы Windows:

– кто имеет доступ к компьютеру;

– какие ресурсы могут использовать пользователи на компьютере;

– включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задание 12. Опишите параметры и значения параметров Политики паролей.

Задание 13. Опишите параметры и значения параметров Политики учетной записи. ***Задание 14.*** 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. Этот пароль является результатом выполнения вашего задания.

Задание 15. После успешного выполнения предыдущего задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

Задание 16. Проведите эксперименты с другими параметрами Политики учетных записей.

Задание 17. Выполните задания.

- Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).

- Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.

- Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

- Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.

- Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

- Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

- Составьте отчет о проведенных экспериментах.

Задание 18. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 1.3.2. Регистрация событий (аудит)., Контроль целостности данных, Уничтожение остаточной информации.

Задание 1. Опишите параметры и значения параметров Политики аудита.

Задание 2. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие данные по каждому событию отображаются в журнале?

Задание 3. Включите аудит успеха и отказа всех параметров.

Задание 4. Выйдите из системы и предпримите попытку входа в операционную систему с неверным паролем. Откройте журнал событий, найдите соответствующую запись.

Задание 5. Удалите раннее созданную учетную запись и зафиксируйте все события системного журнала, связанные с этим действием.

Задание 6. Создать несколько файлов, заполнить их данными. Сделать копии файлов и произвести для некоторых из них «незаметные» для пользователей изменения в файлах. К таким изменениям можно отнести, к примеру:

- изменение кода цвета объектов, в частности текста;
- замена символов на похожие символы с другими кодами символов;
- вставка объектов со 100 %-ной прозрачностью, отсутствующими цветами заливками или совпадающими с цветом фона;
- изменение текста до минимального, установка цвета текста под цвет фона;
- вставка текста с атрибутами «скрытый текст», опция «Шрифт» => «Видоизменение»;
- изменение рисунка (областей с мало отличимой палитрой цветов);
- изменение метаданных файлов (к примеру, вкладка «Подробно» с полями «Авторы», «Организация» и пр.);
- прочее.

Задание 7. Используя программную реализацию механизма хэш-функций, проверить целостность и неизменность файлов. Предоставить снимки экрана, описание действий и результатов. Прокомментировать детально результаты работы: когда совпадают, когда расходятся и почему.

Задание 8. Изучить возможность атаки на хэш-функцию, продемонстрировать пример.

Задание 9. Продемонстрировать возможность тайной передачи данных (картинок, текста) в документах так, чтобы проверка контрольной суммы не обнаружила изменений.

Задание 10. Опишите причины возникновения остаточной информации.

Задание 11. Приведите примеры устройств уничтожения информации с магнитных носителей.

Задание 12. Изучите особенности современных методов ликвидации информации на магнитных носителях. Заполните таблицу.

Метод ликвидации информации	Принцип действия	Основные особенности

Задание 13. Изучите основные особенности современных устройств ликвидации магнитных записей. Заполните таблицу.

Тип устройства	Принцип действия	Основные особенности

Задание 14. Перечислите основные требования к современным устройствам уничтожения информации с магнитных носителей.

Задание 15. Охарактеризуйте программные методы уничтожения информации.

Результаты зафиксировать в отчете.

5. Задание к практическому занятию 1.3.3. Управление политикой безопасности. Шаблоны безопасности, Криптографическая защита. Обзор программ шифрования данных, Управление политикой безопасности. Шаблоны безопасности

Задание 1. Исследуемая система состоит из множества субъектов и объектов.

Исходные данные

СУБЪЕКТЫ

1. Пользователь 1 (Администратор).
2. Пользователь 2.
3. Пользователь 3.
4. Текстовый редактор Word.
5. Редактор формул.
6. Модуль проверки правописания.

ОБЪЕКТЫ

1. Документ пользователя 1.
2. Документ пользователя 2.
3. Документ пользователя 3.
4. Файл текстового редактора Word WINWORD.EXE.
5. Файл редактора формул EQUATION.DLL.
6. Файл модуля проверки правописания SPELL.DLL.
7. Файл-словарь DICTIONARY.DOC.

Политика безопасности системы устанавливает следующий порядок работы, при котором:

– пользователь 1 имеет возможность работы со своим документом с помощью программы WORD, может только просматривать документы пользователя 2 и 3, может проверять правописание в своем документе и вставлять в него формулы. Так же пользователь 1 может добавлять новые слова в словарь;

– пользователь 2 имеет возможность работать только со своим документом, может проверять правописание, но не может добавлять новые слова в словарь и не может вставлять в документ формулы;

– пользователь 3 имеет возможность работать со своим документов и документом пользователя 2, может проверять правописание в обоих документах, может добавлять в документы формулы, но не может добавлять новые слова в словарь.

Программа Word может быть запущена только пользователями системы и может вызывать редактор формул и модуль проверки правописания.

Только модуль проверки правописания может изменять файл-словарь DICTIONARY.DOC.

Необходимо:

– составить множество возможных прав доступа в системе. Для заданного множества субъектов и объектов построить матрицу доступов и заполнить ее в соответствии заданной политикой безопасности и с принципом минимизации привилегий;

– дополнить матрицу доступов временными доменами (например, добавить строку "Программа Word, запущенная от имени первого пользователя" или "Редактор формул, запущенный третьим пользователем из программы Word"). В матрице доступов должны быть представлены временные домены для всех возможных комбинаций взаимодействующих субъектов.

Задание 2. Заданы документы с различным уровнем секретности, заданы пользователи с различным уровнем доступа (список документов и пользователей и их уровни доступа/секретности составить самостоятельно. Не менее 5 пользователей и 5 документов).

1. Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

2. Для одного из пользователей составить список документов, доступных ему для работы при условии, что пользователь может понизить свой уровень доступа на один уровень.

3. Один из пользователей имеет возможность работать с несколькими документами. На основе этих документов он создает новый документ. Какой гриф секретности нужно присвоить этому документу?

4. Показать на примере одного из пользователей, что мандатная политика безопасности не может быть нарушено программой типа "Троянский конь".

Задание 3. Разработать алгоритм шифрования данных.

Задание 4. Привести примеры программ шифрования данных.

Задание 5. Провести сравнительный анализ программ шифрования данных.

Задание 6. Описать возможности одной из программ шифрования данных.

Задание 7. Загрузите редактор Шаблона безопасности. В каком месте на диске хранятся (по умолчанию) шаблоны безопасности?

Задание 8. Отредактируйте шаблон безопасности и сохраните его под новым именем.

Задание 9. Опишите разделы, включаемые в стандартный Шаблон безопасности.

Задание 10. Опишите, какие параметры политики безопасности можно настроить с помощью

шаблонов безопасности?

Результаты зафиксировать в отчете.

6. Задание к практическому занятию 1.4.1. Распределение каналов в соответствии с источниками воздействия на информацию

Практическое занятие 1.4.1.Распределение каналов в соответствии с источниками воздействия на информацию

Задание 1. Заполнить таблицу:

Канал связи	Среда	Носитель сообщения	процесс, используемый для передачи сообщения
Почта, курьеры			
Телефон, компьютерные сети			
Радио, телевидение			
Зрение			
Слух			
Обоняние, вкус			
Осязание			

Задание 2. Приведите конкретные примеры каналов несанкционированного получения информации каждого класса. Классы каналов несанкционированного получения информации:

1) от источника информации при несанкционированном доступе (НСД) к нему;
2) от средств обработки информации при НСД к ним;
3) от источника информации без НСД к нему;
4) от средств обработки информации без НСД к ним.

Задание 3. Поясните модель канала утечки информации

Задание 4. Провести 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.

Результаты зафиксировать в отчете.

7. Задание к практическому занятию 1.5.1. Организация доступа к файлам

Задание 1. Заполните таблицы.

Разрешения папок NTFS

Разрешения папок NTFS	**Позволяет**
Read (Чтение)	
Write (Запись)	
List Folder Contents (Список содержимого папки)	
Read & Execute (Чтение и выполнение)	
Modify (Изменить)	
Full Control (Полный доступ)	

Разрешения файлов NTFS

Разрешения файлов NTFS	**Позволяет**
Read (Чтение)	
Write (Запись)	
Read & Execute (Чтение и выполнение)	
Modify (Изменить)	
Full Control (Полный доступ)	

Элементы вкладки Security (Безопасность)

Элемент	**Описание**
Name (Имя)	
Permissions (Разрешения)	
Add (Добавить)	
Delete (Удалить)	
Advanced (Дополнительно)	

Задание 2. Планирование разрешений NTFS.

1. Спланируйте разрешения доступа к папкам и файлам. Затем реализуйте разрешения NTFS для файлов и папок вашего компьютера, а затем проверьте назначенные разрешения NTFS и убедитесь, что они работают должным образом.

Перед выполнением упражнений создайте следующие учетные записи и группы:

User8l (нет пароля) — член группы Managers;

User82 (нет пароля) — член группы Accounting;

User83 (нет пароля) — член группы Managers и группы Accounting;

User84 (нет пароля) — не является членом групп Accounting и – Managers.

Создайте следующие папки:

C:\Public;

C:\Public\Library;

C:\Public\Manuals;

C:\Public\Library\Misc.

Можно использовать и свою структуру объектов, имеющихся на вашем компьютере.

2. Спланируйте назначение разрешений NTFS для файлов и папок:

Имя папки	**Группа**	**Разрешения**
Public	Users Administrators	Read & Execute Full Control
Public \ Library	Users Administrators Manager	Read & Execute Full Control Modify
Public \ Library\Misc	Users Administrators User82	Read & Execute Full Control Modify
Public \ Manuals	Users Administrators Accounting	Read & Execute Full Control Modify

Задание 3. Проверка разрешений NTFS.

1. Зарегистрируйтесь в системе под разными учетными записями и проверьте разрешения NTFS.

2. Проверьте разрешения доступа к папке Misc для пользователя User81.

3. Проверьте разрешения доступа к папке Misc для пользователя User82.

4. Зарегистрируйтесь в системе как User82 и откройте папку Public\Library\Misc. Попробуйте создать файл в папке Misc. Удалось ли это? Почему?

5 Проверьте разрешения доступа к папке Manuals для пользователя Administrator. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

6. Проверьте разрешения доступа к папке Manuals для пользователя User81. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

7. Проверьте разрешении доступа к папке Manuals для пользователя User82. Попробуйте создать файл в папке Manuals. Удалось ли это? Почему?

Результаты зафиксировать в отчете.

8. Задание к практическому занятию 1.5.2. Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД

Задание 1. Охарактеризуйте программно-аппаратные средства защиты автоматизированных систем от НСД.

Задание 2. В качестве примеров отдельных программ, повышающих защищенность от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации

при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др. Опишите одно из программных средств, повышающих защищенность от НСД.

Задание 3. В качестве примеров отечественных аппаратно-программных средств защиты можно привести системы «Аккорд-4», «DALLAS LOCK 3.1», «Редут», «ДИЗ-1».Опишите одно из программно-аппаратных средств защиты информации от НСД.

Задание 4. Приведите примеры современных систем защиты ПК от несанкционированного доступа к информации.

Результаты зафиксировать в отчете.

10. Задание к практическому занятию 2.4.1. Защита информации от несанкционированного копирования с использованием специализированных программных средств. Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)

Задание 1. Охарактеризуйте программно-аппаратные средства защиты автоматизированных систем от НСД.

Задание 2. В качестве примеров отдельных программ, повышающих защищенность от НСД, можно привести утилиты из пакета Norton Utilities, такие как программа шифрования информации

при записи на диск Diskreet или Secret disk, программа стирания информации с диска WipeInfo, программа контроля обращения к дискам DiskMonitor и др. Опишите одно из программных средств, повышающих защищенность от НСД.

Задание 3. В качестве примеров отечественных аппаратно-программных средств защиты можно привести системы «Аккорд-4», «DALLAS LOCK 3.1», «Редут», «ДИЗ-1».Опишите одно из программно-аппаратных средств защиты информации от НСД.

Задание 4. Приведите примеры современных систем защиты ПК от несанкционированного доступа к информации.

Результаты зафиксировать в отчете.

9. Задание к практическому занятию 2.3.1. Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО

Задание 1. Опишите разделы реестра Windows. Заполните таблицы.

Задание 2. В каких разделах реестра хранится информация о выбранной политике безопасности.

Задание 3. Опишите возможности программы REGEDIT.EXE.

Задание 4. Проведите исследование реестра Windows для нахождения следов активности вредоносного ПО.

Результаты зафиксировать в отчете.

11. Задание к практическому занятию 2.5.1. Применение средства восстановления остаточной информации на примере Foremost или аналога

Задание 1. Приведите примеры программ восстановления данных. Опишите их возможности. Составьте сравнительную характеристику.

Задание 2. Опишите возможности программы восстановления данных Foremost. Как Foremost восстанавливает файлы? Опишите параметры запуска программы Foremost.

Задание 3. Создайте произвольный каталог и запишите туда данные каталога другого каталога. Удалите созданный каталог. С помощью Foremost восстановите данные.

Результаты зафиксировать в отчете.

12. Задание к практическому занятию 2.5.2. Применение специализированного программно средства для восстановления удаленных файлов

Задание 1. Опишите назначение и возможности программы Easy Recovery Pro.

Задание 2. Создайте на рабочем столе файл. Удалите его в Корзину. Восстановите файл из Корзины.

Задание 3. Создайте текстовый файл на диске D: с именем Proba.txt, введите свою фамилию, закройте и сохраните файл. Удалите созданный файл. Очистите Корзину. Восстановите файл с помощью программы Easy Recovery Pro.

Задание 4. Создайте на диске D:\ папку с именем Директория. Перепишите в созданную папку с диска C:\ файл Proba.txt. Удалите папку Директория. Очистите Корзину. Восстановите папку с помощью Easy Recovery Pro.

Результаты зафиксировать в отчете.

13. Задание к практическому занятию 2.5.3. Применение программ для безвозвратного удаления данных

Задание 1. Опишите программные механизмы удаления данных. Достоинства и недостатки. На чем основаны программные методы гарантированного удаления информации?

Задание 2. Опишите механические механизмы удаления данных. Как работают аппаратные средства гарантированного удаления информации?

Задание 3. Сравните программные и аппаратные средства гарантированного удаления информации.

Задание 4. Проконтролируйте удаление файла с помощью стандартного метода удаления. Реализовать восстановление файла, после удаления стандартными средствами ОС.

Задание 5. Изучите методы уничтожения данных с электронных носителей путем многократной перезаписи.

Задание 6. В состав программ PGP и BestCrypt входят утилиты для безвозвратного удаления данных. В PGPtools – это Wipe (удаление файлов) и Freespace Wipe (очистка диска). В BestCrypt –Wipe drive free space (очистка диска). Изучите возможности этих утилит.

Задание 7. Создайте на диске D:\ папку с именем Директория. Перепишите в созданную папку с диска C:\ файл Proba.txt. Удалите файл с помощью утилиты Wipe.

Результаты зафиксировать в отчете.

14. Задание к практическому занятию 2.5.4. Применение программ для шифрования данных на съемных носителях

Задание 1. Создайте на диске C:\Темп папку и скопируйте в нее любой файл. Зашифруйте файл вместе с папкой таким образом, чтобы все помещаемые в папку файлы тоже шифровались (если шифрование не удалось – дальнейшие действия с папкой делайте, как с зашифрованной). Создайте на рабочем столе папку с вашей фамилией и добавьте в неё резервную копию зашифрованной вами папки (сохраняя шифрование).

Задание 2. Программа VeraCrypt позволяет создавать виртуальный зашифрованный диск, представляющий собой файл, который можно смонтировать в локальный диск. Программа NeoCrypt позволяет шифровать содержимое файла без изменения его расширения. Опишите возможности этих программ.

Задание 3. Опишите технологию шифрования дисков BitLocker. Примените технологию BitLocker To Go к Flash – диску с пошаговым описанием всех действий. Дайте сравнительную характеристику шифрования жесткого и съемного дисков.

Результаты зафиксировать в отчете.

15. Задание к практическому занятию 2.7.1. Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений

Задание 1. Выделяют следующие методы обнаружения вторжений:

– сигнатурный анализ:

– использование статистики Байеса;

– продукционные (экспертные) системы;

– анализ перехода системы из состояния в состояние и сети Петри;

– статистический анализ:

– относительная частота последовательностей;

– модель среднего значения и среднеквадратичного отклонения;

– операционная модель;

– модель временных серий.

Опишите один из методов обнаружения вторжений.

Задание 2. Поясните классификацию систем обнаружения вторжений.

Задание 3. Охарактеризуйте основные элементы локальной архитектуры систем обнаружения вторжений.

Задание 4. Приведите примеры систем обнаружения вторжений. Охарактеризуйте одну из систем обнаружения вторжений.

Задание 5. Изучите систему обнаружения вторжений Snort

Результаты зафиксировать в отчете.

16. Задание к практическому занятию 3.2.1 Развертывание VPN

Задание 1. Опишите этапы создания VPN сервера в Windows.

Задание 2. Опишите этапы создания VPN клиента в Windows.

Задание 3. Опишите технологии тестирования виртуальных сетей.

Задание 4. Представьте проект виртуальной сети для заданной организации.

Результаты зафиксировать в отчете.

17. Задание к практическому занятию 4.1.1. Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. Изучение различных способов закрытия "опасных" портов

Задание 1. Изучить основные типы архитектур мультихостовых Firewall: Dual Homed Host, Bastion Host, Perimetr, Demilitarized Zone.

Задание 2. Сравнить основные типы архитектур мультихостовых Firewall: Dual Homed Host, Bastion Host, Perimetr, Demilitarized Zone. Результаты представить с помощью таблицы.

Задание 3. Многочисленные исследования и опросы специалистов показывают, что до 80 % вредоносных атак и взломов происходили при помощи четырех основных портов, использующихся для быстрого обмена файлами между разными версиями Windows:

– TCP порт 139;
– TCP порт 135;
– TCP порт 445;
– UDP порт 137.

Пишите назначение приведенных портов.

Задание 4. С помощью командной строки закрыть порты 135-139 и 445.

Задание 5. Опишите назначение и возможности программы Windows Doors Cleaner.

Результаты зафиксировать в отчете.

18. Задание к практическому занятию 5.1.1. Изучение механизмов защиты СУБД MS Access. Изучение штатных средств защиты СУБД MSSQL Server

Задание 1. Создать новую базу данных и создать в ней следующие объекты:

- таблицу Заказы;
- запрос Сведения о заказах;
- форму Заказы клиентов.

Заполнить таблицу несколькими записями.

Задание 2. Защитите созданную базу данных паролем. Каким образом обеспечивается целостность данных?

Задание 3. Защитите созданную базу данных с помощью Мастера. MS Access предоставляет

средства распределенного доступа к базе данных. С одним файлом могут одновременно работать большое количество пользователей, обладающих разными правами: одни могут только просматривать таблицы, другие – только вносить новые данные, и лишь администраторы базы обладают полным доступом. Разделите доступ для двух пользователей – один сможет только просматривать данные (читать), другой будет обладать полным доступом.

Опишите этапы защиты базы данных с помощью Мастера.

Задание 4. Создайте резервную копию базы данных.

Задание 5. Создать базу данных для работы компьютерных курсов (рисунок 1). Заполнить таблицу несколькими записями.

Задание 6. Установите права на доступ к объектам базы данных.

Задание 7. Каким образом обеспечивается целостность данных?

Задание 8. Изучите операторы GRANT и REVOKE, используемые для предоставления и отмены привилегий соответственно.

Задание 9. Создайте резервную копию базы данных.

Результаты зафиксировать в отчете.

19. Задание к практическому занятию 6.1.1. Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов.

Задание 1. Поясните структуру системы мониторинга информационной безопасности.

Задание 2. Изучите назначение и основные возможности сетевых мониторов (RealSecure, SNORT, NFR или другие аналоги).

Задание 3. Проведите сравнительный анализ распространенных сетевых мониторов. Результаты оформите с помощью таблицы.

Результаты зафиксировать в отчете.

20. Задание к практическому занятию 6.1.2. Проведение аудита ЛВС сетевым сканером

Задание 1. Приведите примеры сканеров безопасности сетевых сервисов и протоколов.

Задание 2. Опишите возможности сетевого сканера безопасности Shadow Security Scanner или аналога. Основные команды.

Задание 3. Перечислите и охарактеризуйте стандартные правила, определяющие параметры сессии сканирования. На базе одного из них создайте собственное правило.

Задание 4. Проведите сканирование указанных преподавателем компьютеров в учебной лаборатории. При сканировании надо учитывать, что часть имеющихся уязвимостей может быть закрыта путем использования встроенного межсетевого экрана (брандмауэра Windows), появившегося в ОС семейства Windows, начиная Windows XP. Чтобы получить более полную информацию об исследуемых узлах, лучше провести одно сканирование при включенном, другое –при отключенном межсетевом экране (изменение настройки доступно через Панель управления –>Брандмауэр Windows). Аналогичная ситуация возникает и при использовании других межсетевых экранов. Опишите результаты проверки – полученные данные о компьютере и сетевых службах, наиболее серьезные из обнаруженных уязвимостей и пути их устранения. Охарактеризуйте уровень безопасности проверенных компьютеров.

Результаты зафиксировать в отчете.

21. Задание к практическому занятию 6.2.1. Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.

Задание 1. Приведите примеры законодательных мер защиты информации в ИС.

Задание 2. Приведите примеры административных мер защиты информации в ИС.

Задание 3. Приведите примеры процедурных мер защиты информации в ИС.

Задание 4. Приведите примеры программно-технических мер защиты информации в ИС.

Задание 5. Разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты:

1. Общие положения.

1.2. Цели системы информационной безопасности.

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности.

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы.

3. Механизмы обеспечения информационной безопасности Предприятия.

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия.

4.1. Организационное обеспечение информационной безопасности:

- задачи организационного обеспечения информационной безопасности;
- подразделения, занятые в обеспечении информационной безопасности;
- взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия:

• общие положения;
• защита информационных ресурсов от несанкционированного доступа;
• средства комплексной защиты от потенциальных угроз;
• обеспечение качества в системе безопасности;
• принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия:
• правовое обеспечение юридических отношений с работниками Предприятия;
• правовое обеспечение юридических отношений с партнерами Предприятия;
• правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

Вариант – номер по списку в таблице

Номер варианта	**Организация**
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Основные принципы программной и программно-аппаратной защиты информации

Тема 1.1. Предмет и задачи программно-аппаратной защиты информации

1. Основные задачи программно-аппаратной защиты информации состоят в: (выбрать все верные)
- обеспечении компьютерной безопасности
- предотвращение утечки информации;
- предотвращение несанкционированного доступа к информации.

2. Предметом рассмотрения и внимания при создании программно-аппаратных методов и средств защиты информации является (выбрать все верные):
- Информация
- Информационная инфраструктура
- Сетевая инфраструктура
- Хранилища данных
- Политика информационной безопасности

3. Чем характерны задачи программно-аппаратной защиты информации (выбрать все верные):

- данный тип задач является четко формализуемым
- большое количество факторов, влияющих на построение эффективной защиты;
- отсутствие точных исходных входных данных;
- отсутствие математических методов получения оптимальных результатов по совокупности исходных данных

4. Программно-аппаратная защиты информации требует знаний в следующих предметных областях: (выбрать все верные):

- программирование
- криптография
- аппаратное обеспечение средств вычислительной техники
- компьютерные сети
- физика
- химия

5. Предметами исследования и изучения при проектировании средств программно-аппаратных средств защиты информации являются (выбрать все верные):

- психология
- физические процессы
- нейронные сети и их алгоритмы
- теория вероятности и рисков
- теория струн

Тема 1.2. Стандарты безопасности

1. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

- Список стандартов, процедур и политик для разработки программы безопасности
- Текущая версия ISO 17799
- Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
- Открытый стандарт, определяющий цели контроля

2. Для кого проявляются преимущества от введения стандартов в области ИБ (выбрать все верные):

- производителей средств обеспечения ИБ
- экспертов в области ИБ
- потребителей средств обеспечения ИБ
- бизнес-руководства предприятий

3. Стандарты в области информационной безопасности выполняют следующие важнейшие функции: (выбрать все верные)

- выработка понятийного аппарата и терминологии в области информационной безопасности
- формирование шкалы измерений уровня информационной безопасности
- согласованная оценка продуктов, обеспечивающих информационную безопасность
- повышение технической и информационной совместимости продуктов, обеспечивающих ИБ
- обеспечение защиты информации, объектов, данных
- функция нормотворчества – придание некоторым стандартам юридической силы и установление требования их обязательного выполнения.

4. Основными областями стандартизации информационной безопасности являются (выбрать все верные):

- аудит информационной безопасности
- модели информационной безопасности
- методы и механизмы обеспечения информационной безопасности

- криптография
- безопасность межсетевых взаимодействий
- управление информационной безопасностью.
- производство средств обеспечения ИБ

5. Какой из стандартов является одним из наиболее известных стандартов, источником лучших практик при построении систем управления информационной безопасностью:

- ГОСТ Р 57580.1-2017
- ГОСТ Р 57580.2-2018
- ГОСТ Р ИСО/МЭК 27001-2006 (ISO/IEC 27001:2013)

Тема 1.3. Защищенная автоматизированная система

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

- Информационная защита информации
- Информационная безопасность
- Зашита информации

2. Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:

- SSL
- SET
- HTTP
- IPSec

3. Программные средства обеспечивают состояние защищенности ИС на основе:

- с помощью шифрования (криптографии)
- методом физического заграждения
- с помощью охранной сигнализации
- с помощью патентной защиты

4. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

- уязвимость информации
- надежность информации
- защищенность информации
- безопасность информации

5. По документам контролирующих органов количество классов защищенности автоматизированных систем от несанкционированного доступа:

- 8
- 7
- 9
- 6

Тема 1.4. Дестабилизирующее воздействие на объекты защиты

1. К источникам дестабилизирующего воздействия на информацию относятся: (выбрать все верные)

- люди;
- технические средства отображения (фиксации), хранения, обработки, воспроизведения, передачи информации,
- средства связи;
- природные явления.
- политическая и экономическая обстановка
- технологические процессы отдельных категорий промышленных объектов

2. Виды и способы дестабилизирующего воздействия на защищаемую информацию дифференцируются по:

- источнику воздействия

- объекту воздействия
- уровню воздействия

3. Со стороны людей возможны следующие виды дестабилизирующего воздействия, приводящие к уничтожению, искажению и блокированию информации: (выбрать все верные)

- Непосредственное воздействие на носители защищаемой информации.
- Несанкционированное распространение конфиденциальной информации.
- Вывод из строя технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи.
- Использование средств компьютерной техники для задач, не предусмотренных должностными инструкциями.
- Нарушение режима рабочего времени

4. К условиям, создающим возможность для дестабилизирующего воздействия на информацию, можно отнести: (выбрать все верные)

- недостаточность мер, принимаемых для защиты информации, в том числе из-за недостатка ресурсов;
- недостаточное внимание и контроль со стороны администрации вопросам защиты информации;
- принятие решений по производственным вопросам без учета требований по защите информации;
- плохие отношения между сотрудниками и сотрудников с администрацией.
- низкая зарплата сотрудников
- некачественный подбор персонала

5. Причинами дестабилизирующего воздействия на информацию со стороны технических средств отображения, хранения, обработки, воспроизведения, передачи информации и средств связи могут быть: (выбрать все верные)

- недостаток или плохое качество средств;
- низкое качество режима функционирования средств;
- перезагруженность средств;
- низкая квалификация персонала, выполняющего настройку и внедрение вышеуказанных средств

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

1. Какие существуют основные группы программно-аппаратных средства защиты информации: (выбрать все верные)

- Средства, разработанные для защиты информации от НСД в информационных сетях, но допускающие применение и в персональных компьютерах;
- Средства НСД на физическом уровне;
- Средства, принципиально предназначенные для защиты информации от НСД в персональных компьютерах.

2. Укажите средства защиты от НСД в информационных сетях (выбрать все верные)

- система защиты от НСД «Спектр-Z»;
- система Secret Net;
- программно-аппаратный комплекс защиты DAALLAS LOCK;
- программно-аппаратная система «Криптон-Вето»;
- система криптографической защиты информации «Верба-0»;
- Ru-token / E-token

3. Принцип работы программно-аппаратной системы КРИПТОН заключается в следующем:

- разбиение жесткого диска на разделы, каждому из которых назначаются права доступа
- доступ к компьютеру осуществляется с помощью биометрического датчика
- текст на экране компьютера шифруется для посторонних, а виден только авторизованному сотруднику

4. Система криптографической защиты информации (СКЗИ) «Верба-0» решает следующие задачи: (выбрать все верные)

- шифрование/расшифрование информации на уровне файлов;
- генерацию электронной цифровой подписи (ЭЦП);
- проверку (ЭЦП).
- создание VPN-канала

5. Основные функции, выполняемые программно-аппаратными средствами защиты от НСД являются:

- идентификация и аутентификация пользователей и устройств;
- регистрация запуска (завершения) программ и процессов;
- управление информационными потоками между устройствами;
- учет носителей информации и другие функции.
- уничтожение информации в случае НСД к ней

Раздел 2. Защита автономных автоматизированных систем

Тема 2.1. Основы защиты автономных автоматизированных систем

1. При использовании Flash-Bios в автоматизированных рабочих местах на базе автономных ПЭВМ необходимо обеспечить:

- форматирование Flash-Bios после обработки
- открытие Flash-Bios на запись
- доступность информации, записанной на Flash-Bios
- целостность информации, записанной на Flash-Bios

2. Какое средство защиты позволяет выявлять несанкционированный доступ (или попытки несанкционированного доступа) к ресурсам автономной автоматизированной системы?

- IDS
- антивирус
- СКД

3. Автономная автоматизированная система должна обеспечивать (выбрать все верные):

- надежность
- четко ограниченную доступность
- целостность
- полную контролируемость в любой момент времени
- интегрированность

4. Укажите основные аспекты защиты автономных систем: (выбрать все верные)

- сетевой
- антивирусный
- защита о НСД
- сохранность информации

5. Укажите программно-аппаратные средства защиты, которые могут использоваться для автономных автоматизированных систем. (выбрать все верные)

- Secret Net LSP,
- Dallas Lock 8.0K,
- Панцирь К",
- Аура 1.2.4.
- ВЕРБА-0
- Secret Net NT

Тема 2.2.Защита программ от изучения

1. В качестве методов защиты программ от изучения используют: (выбрать все верные)

- обфускацию
- встраивание в программу кодов-«пустышек»
- использование частных переменных в коде программы
- использование самогенерируемого кода
- использование полиморфного кода

2. По отношению к каким процессам должна быть устойчива защищенная программа (выбрать все верные):

- дисассемблирование
- работа под контролем отладчика
- архивирование
- шифрование
- компиляция

3. Наиболее известные способы защиты программы от получения кода программы на языке низкого уровня: (выбрать все верные):

- шифрование кода с помощью симметричного ключа
- шифрование кода с помощью асимметричного ключа
- динамическом изменении кода программы в процессе выполнения
- использование нестандартной структуры программы

4. Наиболее известные способы защиты программы от работы под контролем отладчика: (выбрать все верные):

- изменение среды функционирования;
- модификация кодов программы;
- случайные" переходы.
- разделение файла программы на несколько мелких файлов

5. Защищаемая от исследования программа должна включать следующие компоненты: (выбрать все верные):

- инициализатор;
- зашифрованную секретную часть;
- деструктор
- конструктор

Тема 2.3. Вредоносное программное обеспечение

1. Вредоносные программы – это ….

- шпионские программы
- программы, наносящие вред данным и программам, находящимся на компьютере
- антивирусные программы
- программы, наносящие вред пользователю, работающему на зараженном компьютере
- троянские утилиты и сетевые черви

2. К вредоносным программам относятся:

- Потенциально опасные программы
- Вирусы, черви, трояны
- Шпионские и рекламные программы
- Вирусы, программы-шутки, антивирусное программное обеспечение
- Межсетевой экран, брандмауэр.

3. Сетевые черви - это…

Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты, это:

- Вирусы, которые проникнув на компьютер, блокируют работу сети
- Вирусы, которые внедряются в документы под видом макросов
- Хакерские утилиты управляющие удаленным доступом компьютера
- Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

4. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

- Загрузочный вирус;
- Макровирус;
- Троян;
- Сетевой червь;

- Файловый вирус.

5. Вирус поражающий документы называется
- Троян;
- Файловый вирус;
- Макровирус;
- Загрузочный вирус;
- Сетевой червь.

Тема 2.4. Защита программ и данных от несанкционированного копирования

1. Какие основные меры защиты от НСК существуют: (выбрать все верные)
- Организационные
- Юридические
- Технические
- Компьютерные

2. Защита программ, установленных на жёстком диске реализуется в виде: (выбрать все верные):
- необходимость постоянно держать в накопителе носитель информации, например, компакт-диск или флэшку
- использование аппаратного USB или LPT – ключа
- привязка к серийным номерам компонентов компьютера
- сканирование локальной сети на предмет поиска подобной копии программы и блокирования ее
- проверка серийного номера программы через специальный сервер
- генерация уникального пароля при каждом запуске или копировании программы

3. Основные мотивы создания и использования систем защиты от копирования: (выбрать все верные)
- Учет условий распространения программных продуктов
- Учет возможностей пользователей программного продукта по снятию с него системы зашиты
- Учет свойств распространяемого программного продукта
- Оценка возможных потерь при снятии защиты и нелегальном использовании
- Постоянное обновление использованных в системе защиты средств
- Предоставление информации об объеме выпуска копий ПО в органы Госстата, налоговой инспекции
- Учет аппаратного обеспечения, на которое установлено ПО

4. Основные требования, предъявляемые к системе защиты от копирования: (выбрать все верные)
- обеспечение некопируемости дистрибутивных компакт-дисков стандартными средствами;
- обеспечение невозможности применения стандартных отладчиков без дополнительных действий над машинным кодом программы или без применения специализированных программно-аппаратных средств;
- обеспечение некорректного дизассемблирования машинного кода программы стандартными средствами;
- обеспечение сложности изучения алгоритма распознавания индивидуальных параметров компьютера, на котором установлен программный продукт, и его пользователя или анализа применяемых аппаратных средств защиты.
- ограничение на количество запусков программы (или обращений к папке, где установлена программа) в течение суток

5. Каких методов защиты информации от НСК не существует?
- методы, затрудняющие считывание скопированной информации;
- методы, препятствующие использованию информации

- методы, уничтожающие информацию (ПО) при использовании ее неавторизованным лицом

Тема 2.5. Защита информации на машинных носителях

1. Из каких мероприятий состоит процедура защиты машинных носителей информации (ЗНИ) (выбрать все верные):

- Учет машинных носителей информации
- Управление доступом к машинным носителям информации
- Контроль перемещения машинных носителей информации за пределы контролируемой зоны
- Исключение возможности несанкционированного ознакомления с содержанием информации, хранящейся на машинных носителях и /или использования носителей информации в иных информационных системах
- Контроль использования интерфейсов вода - вывода
- контроль ввода – вывода информации на машинные носители
- Контроль подключения машинных носителей информации
- Уничтожение информации на машинных носителях при передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)
- Очистка системного реестра операционной системы после использования защищаемого носителя

2. Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации?

- объект защиты информации
- объект информатизации
- локальная вычислительная сеть
- автоматизированная система

3. Если в АС работает один пользователь, который допущен ко всей информации и эта информация размещена на носителях одного уровня конфиденциальности, такая АС относится к:

- 1 группе
- 2 группе
- 3 группе
- 4 группе

4. Какая информация может использоваться при учете машинных носителей информации? (выбрать все верные)

- регистрационный (учетный) номер носителя.
- идентификационный (серийный) номер носителя, присвоенный производителем
- цвет корпуса носителя
- модель носителя
- вес носителя

5. Какое из программных средств позволяет выполнять поиск остаточной информации на машинных носителях, а также учет носителей:

- Инспектор и Сканер ВС
- АК ВС 2 и AppChecker
- Эшелон

Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей

1. Укажите устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающее маленький пейджер, не присоединяемый к компьютеру и имеющий собственный источник питания:

- Автономный токен
- USB-токен
- Устройство контактной идентификации iButton
- Смарт-карта

- Радиочастотный (RFID) идентификатор
- Бесконтактный идентификатор типа Proximity

2. Какие бывают виды смарт-карт по техническому исполнению (выбрать все верные):
- карты с памятью;
- карты с микропроцессором и памятью
- карты с микропроцессором
- карты без микропроцессора и без памяти

3. Какие устройства могут различаться между собой физически, но выполнять одну и ту же функцию и иметь подобный принцип действия:
- USB-токен и смарт-карта
- Устройство контактной идентификации iButton и автономный токен
- Биометрический сканер и USB-токен
- Биометрический сканер и смарт-карта

4. Какое из устройств может иметь форму миниатюрного калькулятора / флэшки / смарт-карты / брелока:
- Автономный токен
- USB-токен
- Устройство контактной идентификации iButton
- Радиочастотный (RFID) идентификатор
- Бесконтактный идентификатор типа Proximity

5. Укажите системы биометрической идентификации, которые являются наименее затратными (выбрать все верные):
- по узору радужной оболочки и/или сетчатки глаза
- по отпечаткам пальцев
- по геометрической форме руки;
- по форме и размеру лица
- по форме ушей;
- по особенностям голоса
- по анализу ДНК;
- по биомеханическим характеристикам рукописной подписи и / или "клавиатурного почерка"

Тема 2.7. Системы обнаружения атак и вторжений

1. Информация, полученная об информационной атаке может группироваться анализирующим сервером по следующим параметрам: (выбрать все верные)
- IP-адресу атакующего;
- порту получателя;
- номеру агента;
- дате, времени;
- протоколу;
- типу атаки
- IP-адресу атакуемого

2. Протокольные системы обнаружения вторжений используются для….
- Отслеживания трафика
- Отслеживание вирусов
- Отслеживание неисправностей

3. Что не включает архитектура системы обнаружения вторжений?
- Хранилище
- Сенсорную подсистему
- Оперативную память

4. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к…
- Хабу (коммутатору)

- Порту
- Мосту

5. Какого вида системы обнаружения вторжений не существует?

- Гибридная
- Цельная
- Узловая

Раздел 3. Защита информации в локальных сетях

Тема 3.1. Основы построения защищенных сетей

1. Контроль защищенности информационной сети это:

- проверка документации по технике безопасности
- имитация "взлома" информационной сети, осуществляемая силами самой организации или уполномоченными лицами
- установка программно-аппаратных комплексов отслеживания попыток взлома сети
- установка камер видеонаблюдения по маршруту прохождения информационной сети

2. В какой политике безопасности для доступа к любому защищаемому объекту сети применимо запретительное правило: все, что не разрешено явно - запрещено.

- Политике безопасности по умолчанию
- Глобальной политика безопасности
- Стартовой политика безопасности
- Локальной политика безопасности

3. Межсетевой экран в защищенной информационной сети должен

- пропускать пакеты только в одну сторону
- обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи
- осуществлять контроль доступа пользователей внутренней сети
- полностью прекращать доступ между сетями

4. К системам анализа защищенности сети относится:

- Internet Scanner
- BS 7799
- Network IPS
- CRAMM

5. Механизмы защиты, реализованные в межсетевых экранах, серверах аутентификации, системах разграничения доступа, работают ___.

- только на этапе подготовки атаки
- только на этапе завершения атаки
- на всех этапах осуществления атаки
- только на этапе реализации атаки

Тема 3.2. Средства организации VPN

1. При логическом группировании в виртуальных ЛКС используются такие процедуры управления пакетами, как ___ пакетов

- идентификация
- фильтрация
- сортировка

2. На каком уровне строятся наиболее распространенные VPN-системы:

- транспортном;
- прикладном;
- сетевом;
- канальном

3. В виртуальной частной сети реализуется топология:

- любая;
- точка-точка;
- шина;

- в виртуальной частной сети невозможно реализовать топологии.

4. С какой целью часто используются VPN типа «маршрутизатор—маршрутизатор»?

- Для предоставления заказчикам доступа к локальной сети компании.
- Для предоставления служащим доступа к сети компании из их дома.
- Для предоставления доступа к сети компании ее руководителям, находящимся в дороге.
- Для создания соединения между двумя офисами, расположенными на большом расстоянии друг от друга.

5. Аппаратные сети VPN на основе оборудования бывают (Выбрать все верные.):

- сети на основе маршрутизаторов
- сети на основе брандмауэров

Раздел 4. Защита информации в сетях общего доступа *16*

Тема 4.1.Обеспечение безопасности межсетевого взаимодействия

1. Для подключения пользователей к сети компания использует беспроводные технологии. Были разработаны требования безопасности: Обеспечение конфиденциальной передачи данных; обеспечение целостности данных. Какие из перечисленных протоколов позволят решить поставленную задачу? (выбрать все верные):

- ESP
- WEP
- WPA
- 802.1x
- 802.11i

2. Политика безопасности компании запрещает пользователям посещение некоторых сайтов. Адреса сайтов занесены в черные списки, которые периодически обновляются. Кроме того, требуется блокировка любых баннеров. Какой из перечисленных типов брандмауэров позволит реализовать данную политику безопасности?

- Брандмауэр пакетной фильтрации
- NAT
- Брандмауэр уровня приложений
- RADIUS сервер
- PAT

3. В регистрационном журнале сервера обнаружены несколько подобных записей, свидетельствующих о реализации атаки: Jul 8 18:23:20 fender sshd[15019]: Illegal user bruce from 207.232.63.45

Какой тип систем обнаружения атак следует использовать для предотвращения вторжений такого типа в будущем?

- Анализаторы регистрационных файлов
- Анализаторы сетевой активности
- Мониторы регистрационных файлов
- Системы обнаружения атак на сетевом уровне
- Системы контроля целостности

4. Какой из перечисленных протоколов обеспечения сетевой безопасности является частью протокола IPSec и выполняет следующие функции: Обеспечение целостности данных; защита от повторения данных; удостоверение источника данных.

- AH
- MD5
- SNMP
- SSH
- ICV

5. Какой компонент защиты как минимум должен присутствовать в локальных и корпоративных сетях для обеспечения информационной безопасности:

- межсетевой экран

- механизм криптографии
- система обнаружения сетевых атак
- система обнаружения сетевых вторжений

Раздел 5. Защита информации в базах данных

Тема 5.1. Защита информации в базах данных

1. Какая копия базы данных позволяет восстановить информацию полностью на 100% при сбое в любой момент времени?
- Дифференциальная резервная копия
- Резервная копия
- Никакая из копий

2. Самым надежным способом защиты данных от потери является:
- создание кластеров
- резервное копирование данных и журнала транзакций
- резервное копирование
- технологии RAID

3. Верно ли утверждение: модель полного восстановления следует использовать для рабочей базы данных, содержащей критически важные данные?
- да
- нет

4. Верно ли утверждение: простая модель восстановления может использоваться при разработке баз данных или при работе с базами, которые не требуют частого редактирования ?
- да
- нет

5. Виды защиты баз данных (выбрать все верные):
- защита всех учетных записей, защита идентифицированных объектов
- защита учётной записи группы администратора
- приложение, которое используется для управления базой данных
- защита группы Users
- дискреционная защита

Раздел 6. Мониторинг систем защиты

Тема 6.1. Мониторинг систем защиты

1. В каких направлениях можно развивать систему мониторинга действий по защите конфиденциальной информации?
- наращивание функционала
- наращивание аналитических возможностей
- интеграция систем защиты от внутренних и внешних угроз
- построение системы предотвращения утечек

2. Является ли построение системы предотвращения утечек дальнейшим развитием системы мониторинга действий по защите конфиденциальной информации?
- нет, не является
- да, является
- да, но только одновременно с наращиванием аналитических возможностей

3. Мониторингом может являться (выбрать все верные):
- Запись определенных событий в журнал безопасности сервера называется
- Получение и анализ информации о состоянии ресурсов системы с помощью специальных средств контроля называется
- Получение доступа к информации, перехваченной другими программными закладками

4. Механизм подотчётности пользователей, который позволяет выполнять мониторинг нарушений целостности информации, это:
- аудит произошедших событий
- объективный контроль
- управление передачей привилегий

- аутентификация пользователей
- идентификация пользователей

5. Что может включать в себя мониторинг систем защиты информации (выбрать все верные):

- Просмотр журнала событий операционной системы на серверах и рабочих станциях
- Анализ сетевого трафика
- Просмотр записей с камер видеонаблюдения
- Наблюдение за стабильностью электропитания
- Отслеживание финансовых расходов предприятия
- Анализ содержимого носителей информации на серверах и рабочих станциях

Тема 6.2. Изучение мер защиты информации в информационных системах

1. Планирование бесперебойной работы организации относится к ключевым индикаторам в методиках оценки принимаемых мер по обеспечению информационной безопасности:

- нет
- да

2. Подход к анализу и оценке принимаемых мер по обеспечению информационной безопасности основывается на вычислении весовых коэффициентов опасности для источников угроз и уязвимостей:

- да
- нет

3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- Анализ рисков
- Анализ затрат / выгоды
- Результаты ALE
- Выявление уязвимостей и угроз, являющихся причиной риска

4. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

- меры обеспечения целостности;
- административные меры;
- меры обеспечения конфиденциальности.

5. При анализе стоимости защитных мер следует учитывать:

- расходы на закупку оборудования
- расходы на закупку программ
- расходы на обучение персонала

Тема 6.3. Изучение современных программно-аппаратных комплексов.

1. Правила защиты информации – абстрактное описание комплекса программно-технических средств и организационных мер защиты от несанкционированного доступа к информации называется:

- Модель
- Макет
- Прототип
- Концепт

2. Укажите типовые методы изучения современных программно-аппаратных комплексов в условиях учебного заведения (выбрать все верные)

- чтение инструкции, прилагаемой к программно-аппаратному комплексу
- самостоятельное получение навыков в установке и настройке
- проведение лабораторных работ
- чтение форумов в Интернете
- обращение в техподдержку
- самостоятельное моделирование вариантов использования

3. Укажите типовые методы изучения современных программно-аппаратных комплексов в реальных рабочих условиях (выбрать все верные)

- чтение инструкции, прилагаемой к программно-аппаратному комплексу
- самостоятельное получение навыков в установке и настройке
- чтение форумов в Интернете
- обращение в техподдержку
- самостоятельное моделирование вариантов использования

4. Наилучший эффект при изучении программно-аппаратного комплекса достигается при: (выбрать все верные)

- самостоятельном изучении
- наблюдении за специалистом, который имеет опыт в этом вопросе
- обсуждении на форумах
- обучении на специализированных курсах
- все перечисленное

5. При изучении программно-аппаратного комплекса ответственность за его исправность и правильную работу возлагается на: (выбрать все верные)

- производителя
- специалиста, который его настраивает и вводит в эксплуатацию
- специалиста, который будет его использовать
- всех вышеперечисленных

5.2.1.2. МДК.02.02. Криптографические средства защиты информации

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Что такое шифрование?
2. Что такое кодирование?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Введение. Предмет и задачи криптографии. История криптографии. Основные термины.

1. Что такое шифрование?
2. Что такое кодирование?
3. Что изучает криптография?
4. Когда были известны первые алгоритмы шифрования?
5. Что такое криптостойкость?

Раздел 1. Математические основы защиты информации

Тема 1.1. Математические основы криптографии

1. Какую математическую функцию относительно легко вычислить, но трудно найти соответствующее значение аргумента?
2. Какие из разделов математики легли в основу современных методов криптографии?
3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?
4. С каким алфавитом принято работать в теоретической криптографии ?
5. Какие виды математических последовательностей используются в криптографии?

Раздел 2. Классическая криптография

Тема 2.1. Методы криптографического защиты информации

1. Что представляет собой криптографическая система?
2. Что принято называть электронной подписью?
3. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?
4. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях?
5. Как называется криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот?

Тема 2.2. Криптоанализ

1. Какова цель криптоанализа?
2. С использованием каких инструментов позволяет раскрыть секретные сообщения криптоанализ ?
3. От чего зависит секретность сообщения по мнению О. Кирхгоффа?
4. Какие методы криптоанализа применяются для ассиметричных шифров?
5. Какие методы криптоанализа применяются для симметричных шифров?

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел

1. Как поточный шифр выполняет преобразование входного сообщения?
2. Какими свойствами должен обладать генератор псевдослучайных чисел для использования в криптографических целях ?
3. Какой из генераторов псевдослучайных чисел является наиболее простым?
4. Какой алгоритм используется для шифрования паролей в ОС Windows, а также в протоколе SSL?
5. На чем основан принцип действия всех генераторов псевдослучайных чисел?

Раздел 3. Современная криптография

Тема 3.1. Кодирование информации. Компьютеризация шифрования.

1. Что представляет собой кодирование информации?
2. В чем заключается общая идея помехоустойчивого кодирования?
3. Какие коды используются в помехоустойчивом кодировании?
4. Какими свойствами обладает процедура шифрования данных?
5. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?

Тема 3.2. Симметричные системы шифрования

1. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования?
2. Какой алгоритм, использует симметричный ключ и алгоритм хэширования?
3. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?
4. Какой размер ключа в отечественном стандарте симметричного шифрования?

Тема 3.3. Асимметричные системы шифрования

1. В чем основные преимущества и недостатки асимметричных криптосистем?
2. Сколько используется ключей в асимметричных криптосистемах для шифрования и дешифрования?

3. Какими свойствами секретности должны обладать ключи в асимметричных системах шифрования?

4. Какие шифры (механизмы обмена ключами) относятся к асимметричным?

5. Какая связь существует между двумя ключами в асимметричной криптографии?

Тема 3.4. Аутентификация данных. Электронная подпись

1. Какие методы разрабатываются с целью обеспечения аутентификации?

2. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

3. Какие существуют системы аутентификации и распределения ключей?

4. Что принято называть электронной (цифровой) подписью?

5. Что используют для создания цифровой подписи

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

1. Позволяет ли обмениваться ключами по незащищенным каналам связи Метод Диффи-Хеллмана?

2. Применяется ли для распределения ключей между пользователями информационной системы прямой обмен ключами между пользователями сети?

3. Как называют процесс согласования сессионного ключа в процессе информационного обмена ?

4. Какие существуют протоколы аутентификации?

5. Сколько шагов предусматривает аутентификация с помощью протокола Kerberos версии 5 ?

Тема 3.6. Криптозащита информации в сетях передачи данных

1. Что такое линейное шифрование?

2. Какой шифратор можно использовать для защиты передаваемой в Сеть информации?

3. Какой основной механизм обеспечивает конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе по сети Интернет?

4. Какие из приведенных криптографических алгоритмов используют в основе сетей Фейстеля?

5. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?

Тема 3.7. Защита информации в электронных платежных системах

1. Какие механизмы защиты должны быть реализованы для обеспечения функций защиты информации на отдельных узлах электронной платежной системы?

2. Какой протокол передачи данных обеспечивает лучшую защиту в системах электронных платежей?

3. Каковы преимущества и недостатки протокола SSL?

4. Какие ключи используются в протоколе SET?

5. Какой набор функций обеспечивает смарт-карта ?

Тема 3.8. Компьютерная стеганография

1. Что может являться файлом – контейнером для стеганографии?

2. Что такое метод LSB в стеганографии ?

3. Какие принципы лежат в основе стеганографии?

4. Что скрывает стеганография?

5. Что такое стеганографическая система или стегосистема?

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Какие принципы лежат в основе стеганографии?
2. Что скрывает стеганография?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1.Задание к практическому занятию 1.1.1. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений

1. Найти НОД двух натуральных чисел, используя алгоритм Евклида делением
2. Найти НОД двух натуральных чисел, используя алгоритм Евклида вычитанием
3. Решить диофантово уравнение с помощью алгоритма Евклида: 23x+4y-7x=-3y+15

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.1.2. Проверка чисел на простоту

1. Рассмотреть процедуру проверки чисел на простоту с помощью тестов Ферма и Миллера-Рабина.
2. Рассмотреть схему нахождения наибольшего общего делителя с использованием расширенного алгоритма Эвклида.
3. Реализовать программно тест Ферма. Проверить на простоту целые числа в диапазоне [3,200].
4. Реализовать программно тест Миллера-Рабина. Проверить на простоту целые числа в диапазоне [3,200].
5. Реализовать программно расширенный алгоритм Эвклида. Найти наибольший общий делитель чисел, заданных преподавателем. Сделать вывод об их взаимной простоте.

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 1.1.3. Решение задач с элементами теории чисел.

1. После деления двузначного числа на сумму его цифр в частном получается 7, а в остатке 6. После деления этого же числа на произведение его цифр в частном получается 3, а в остатке 11. Найдите это число.
2. Ученик перемножил два данных натуральных числа и допустил ошибку, увеличив произведение на 372. Поделив для проверки полученный результат на меньшее из данных чисел, ученик правильно получил в частном 90 и в остатке 29. Найдите данные числа.

3. На факультет подано от не медалистов на 600 заявлений больше, чем от медалистов. Девушек среди не медалистов больше, чем среди медалистов, в 5 раз, а юношей среди не медалистов больше, чем среди медалистов, в n раз, где n – натуральное число и . Найдите общее число заявлений, если среди медалистов юношей на 20 больше, чем девушек.

4. Ваня задумал простое трехзначное число, все цифры которого различны. На какую цифру оно может оканчиваться, если его последняя цифра равна сумме первых двух.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 2.1.1. Применение классических шифров замены

1. Создать программу, реализующую процесс шифрования/дешифрования текста по следующим алгоритмам: a. аддитивный моноалфавитный шифр с задаваемым смещением; b. мультипликативный моноалфавитный шифр с задаваемым смещением; c. шифр Плейфера. Разрабатываемая подпрограмма использует только алфавит
абвгдеёжзийклмнопрстуфхцчшщъыэюя

2. Провести частотный анализ символов зашифрованного текста для аддитивного и мультипликативного шифров. Вывести полученный числовые значения на экран.

3. С помощью полученной частоты встречаемости символов вручную провести и описать процесс дешифрование первых 15 символов зашифрованного сообщения.

Результаты зафиксировать в отчете.

5. Задание к практическому занятию 2.1.2. Применение классических шифров перестановки

1. Создать программу, реализующую процесс шифрования/дешифрования текста по изученным шифрам перестановки. Разрабатываемая подпрограмма использует только алфавит:

абвгдеёжзийклмнопрстуфхцчшщъыэюя_,.
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЭЮЯ

При использовании шифра перестановки с ключом длина ключа и сам ключ должны задаваться пользователем. Длина исходного текста должна быть не менее 10000 символов.

Подсчет количества символов должен быть осуществлен самой программой и выведен в поле для ввода.

2. Создать подпрограмму, определяющую ключ шифрования для закрытого текста, зашифрованного комбинированным шифром. Правильность подобранного ключа определяется пользователем. Если ключ подобран неверно, то пользователь отвергает его и отправляет команду на подбор следующего значения ключа. Количество символов в зашифрованном тексте никак не ограниченно.

3. Дешифровать закрытые тексты заданий своего варианта. При шифровании использовался шифр с перестановками по ключу. Дешифрование можно выполнить как вручную, так и программно.

Задан шифртекст:

чбюЛтюолянн и з,уаосрон нтоюлбюь вю !
би оНдеепрсе тс аем.о уйдок
а, лНаивсеаул нкнпв,кояю ьр
лй оНыинпо од оггрипврд ояе о,о к й
мй еНоинти тр ыснан втзеаыен еапярьд
вя еНлеешм в те нонордогтоааяет ьмнч

Результаты зафиксировать в отчете.

6. Задание к практическому занятию 2.1.3. Применение метода гаммирования

1. Выберите метод получения гаммы шифра (псевдослучайной последовательности чисел).

2. Реализуйте программный модуль в соответствии с полученным заданием.

При реализации необходимо учесть следующие моменты:

1) предусмотреть возможность задания пользователем гаммы шифра;

2) предусмотреть визуализацию всех пользовательских настроек;

3) для удобства тестирования и взаимодействия с другими модулями реализовать файловый ввод исходных данных и файловый вывод результата криптографического преобразования.

3. После реализации программного модуля выполните статистический анализ текста до криптографического преобразования и после него.

Варианты заданий:

1. Модуль для шифрования текста гаммированием по модулю.
2. Модуль для расшифровывания текста гаммированием по модулю.
3. Модуль для шифрования текста двоичным гаммированием.
4. Модуль для расшифровывания текста двоичным гаммированием.

Результаты зафиксировать в отчете.

7. Задание к практическому занятию 2.2.1. Криптоанализ шифра простой замены методом анализа частотности символов

1. Получить от преподавателя текстовый файл, содержащий большой художественный текст на русском языке в открытом виде.
2. С помощью программы «Частота символов» исследуйте частотность символов открытого теста.
3. Внести полученную статистику в отчет по работе (первые 15-20 символов). Пример отчета приведен на последней странице.
4. Получить от преподавателя текстовый файл, содержащий большой объем зашифрованного текста на русском языке.
5. Исследовать частотность зашифрованного текста и внести ее в отчет в виде, аналогичном пункту 2 (первые 15-20 символов).
6. Сравнивая реальную частотность символов русского языка, полученную в пункте 2, с частотностями зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст, реализовав программу дешифровки. Дешифровке подвергните только первые 15-20 символов, наиболее часто встречающиеся в шифротексте. Сформированную таблицу замен внести в отчет по работе.
7. Выполнить эвристический анализ текста, полученного в результате дешифровки. По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида. Окончательную таблицу замен (с учетом эвристических подмен) внести в отчет по работе.

Результаты зафиксировать в отчете.

8. Задание к практическому занятию 2.2.2. Криптоанализ классических шифров методом полного перебора ключей

1. Выбрать шифротекст для своего варианта
2. Сформировать таблицу биграмм для эталонного текста на русском языке
3. Разработать программу для полного перебора ключей длины 3 в шифре Виженера и оценки вероятности для каждого расшифрованного исходного текста
4. Найти 10 расшифрованных строк с самой большой оценкой вероятности
5. Расшифровать шифротекст

Результаты зафиксировать в отчете.

9. Задание к практическому занятию 2.2.3. Криптоанализ шифра Вижинера

Используем Excel.

1. Выбрать значение ключа шифрования и криптограмму из табл. 1.10 в соответствии с номером варианта (от 1 до 26).
2. Расшифровать криптограмму выбранным ключом:

3. ввести текст криптограммы побуквенно в ячейки строки отформатированной области; важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;

4. строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР;

5. строкой ниже сформировать ключевую строку;

6. строкой ниже получить числовой код символов ключевой строки с помощью функции ВПР;

7. строкой ниже получить код символа открытого текста, вычтя по модулю 33 код текущего символа ключевой строки из кода текущего символа криптограммы, используя функцию ОСТАТ (рис. 1.44);

8. строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид. Критерием правильности расшифрования является получение осмысленного слова.

Результаты зафиксировать в отчете.

<u>10. Задание к практическому занятию 2.3.1. Применение методов генерации ПСЧ</u>

Требуется Excel

1. Выбрать значения параметров BBS-генератора p, q и случайное число s согласно номеру варианта. Сформировать псевдослучайную последовательность.

2. В приложении MS Excel создать новую книгу, на первом листе ввести значения p, q, вычислить число Блюма n как их произведение, например =B1*B2. Ниже ввести значение случайного числа x.

3. Рассчитать элементы ряда x': • пронумеровать ячейки первого столбца от 0 до 7; • в первую ячейку второго столбца ввести формулу для вычисления x0 по формуле x0 = s'2 mod и, например =ОСТАТ(B4Л2;B3); • скопировать формулу на весь ряд.

4. Вычислить младшие биты чисел xr Значение младшего бита определяется остатком от деления числа на 2, поэтому для вычисления можно использовать функцию ОСТАТ, например =ОСТАТ(B5;2) для числа x0. Скопировать формулу на все ячейки диапазона.

5. Сформировать результирующую битовую псевдослучайную последовательность с помощью операции &, например =C5&C6&C7&C8&C9&C10& C11&C12, или функции СЦЕПИТЬ из группы Текстовые, например =СЦЕПИТЬ(C5;C6;C7;C8;C9;C10;C11;C12). Значение результирующей последовательности: 11101111.

Результаты зафиксировать в отчете.

<u>11. Задание к практическому занятию 3.1.1. Кодирование информации</u>

1. Закодируйте свое имя, фамилию и отчество с помощью одной из таблиц (win-1251, KOI-8)

2. Раскодируйте ФИО соседа

3. Закодируйте следующие слова, используя таблицы ASCII-кодов: ИНФОРМАТИЗАЦИЯ, МИКРОПРОЦЕССОР, МОДЕЛИРОВАНИЕ

4. Раскодируйте следующие слова, используя таблицы ASCII-кодов:

88 AD E4 AE E0 AC A0 E2 A8 AA A0

50 72 6F 67 72 61 6D

43 6F 6D 70 75 74 65 72 20 49 42 4D 20 50 43

5. Текстовый редактор Блокнот

- Используя клавишу Alt и малую цифровую клавиатуру раскодировать фразу: 145 170 174 224 174 255 170 160 173 168 170 227 171 235;

Технология выполнения задания: При удерживаемой клавише Alt, набрать на малой цифровой клавиатуре указанные цифры. Отпустить клавишу Alt, после чего в тексте появится буква, закодированная набранным кодом.

- Используя ключ к кодированию, закодировать слово – зима;

Технология выполнения задания: Из предыдущего задания выяснить, каким кодом записана буква а. Учитывая, что буквы кодируются в алфавитном порядке, выяснить коды остальных букв.

6. Текстовый процессор MS Word.

Технология выполнения задания: рассмотрим на примере: представить в различных кодировках слово Кодировка

- Создать новый текстовый документ в Word;
- Выбрать – Команда – Вставка – Символ.
- В открывшемся окне «Символ» установить из: Юникод (шестн.),
- В наборе символов находим букву К и щелкнем на ней левой кнопкой мыши (ЩЛКМ).
- В строке код знака появится код выбранной буквы 041А (незначащие нули тоже записываем).
- У буквы о код – 043Е и так далее: д – 0434, и – 0438, р – 0440, о – 043Е, в – 0432, к – 043А, а – 0430.
- Установить Кириллица (дес.)
- К – 0202, о – 0238, д – 0228, и – 0232, р – 0240, о – 0238, в –0226, к – 0202, а –0224.

7. Открыть Word.

- Используя окно «Вставка символа» выполнить задания: Закодировать слово Forest
- Выбрать шрифт Courier New, кодировку ASCII(дес.) Ответ: 70 111 114 101 115 116
- Выбрать шрифт Courier New, кодировку Юникод(шест.) Ответ: 0046 006F 0072 0665 0073 0074
- Выбрать шрифт Times New Roman, кодировку Кирилица(дес.) Ответ: 70 111 114 101 115 116
- Выбрать шрифт Times New Roman, кодировку ASCII(дес.) Ответ: 70 111 114 101 115 116

Результаты зафиксировать в отчете.

12. Задание к практическому занятию 3.1.2. Программная реализация классических шифров

1. Разработать программу для шифрования и расшифровывания текста при помощи шифра перестановки или шифра замены. Программа должны обеспечивать:

- задание в командной строке режима работы (шифрование/расшифрование), имени входного файла, имени результирующего файла;
- ввод ключа шифрования/расшифрования с клавиатуры;
- шифрование информации, находящейся в текстовом файле, с записью результата в другой файл.

2. Зашифровать и расшифровать файл, с использованием разработанной программы.

Результаты зафиксировать в отчете.

13. Задание к практическому занятию 3.1.3.Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.

1. Для выполнения работы запускаем программу L_Lux.exe. После открытия главного окна программы определяем установленное в программе смещение для одноалфавитного метода с фиксированным смещением. При определении смещения после шифрования на гистограмме видно строка считывается побуквенно и каждый символ имеющийся в этой строке увеличивается на 3. То есть а+3=г. Дешифрование происходит так же, как и шифрование только зашифрованная строка считывается побуквенно, представляется в массив и каждый элемент массива подменяется на другой элемент: а=г-3.

2. Для одноалфавитного метода шифрования с заданным смещением зашифровать, расшифровать текст и сравнить гистограммы. Расшифровка текста методом подбора смещения. Определим смещение методом подбора смещения для дешифрования исходного текста.

Искомый текст (смещение 8)

Дешифрование методом подбора (смещение 6)

Дешифрование методом подбора (смещение 4)

Дешифрование методом подбора (смещение 2)

3. Дешифровать зашифрованный текст методом постановки, вычислить закономерность перестановки символов. Данный метод заключается в том, что вся строка разбивается на блоки (от 1 до 9 символов) и символы в каждом блоке располагаются в определенной последовательности. В данном случае строка разбилась на блоки по 2 символа которые расположены в порядке 2 символ 1 символ.

4. Инверсное кодирование (по дополнению до 255). Как показано на рисунке нижу будет зашифрован данный текст (данная строка). Инверсный метод потому, что все символы строки обрабатываются и выводятся в обратном порядке как показано на диаграмме выше. Данный метод шифрования, является частным случаем одноалфавитной замены в алфавите мощности 256. Суть метода заключается в замене символа ASCII-кодировки с номером i на символ с номером 255-i. Аналогично проводится и операция дешифрования.

Результаты зафиксировать в отчете.

14. Задание к практическому занятию 3.2.1. Изучение программной реализации современных симметричных шифров

1.Ознакомьтесь с теоретическими основами блочного симметричного шифрования в конспектах лекций.

2.Получите вариант задания у преподавателя.

3.Напишите программу согласно варианту задания.

4.Отладьте разработанную программу и покажите результаты работы программы преподавателю.

Содержание отчета

- название и цель работы;
- вариант задания;
- листинг разработанной программы с комментариями;
- результаты работы программы.

Результаты зафиксировать в отчете.

15. Задание к практическому занятию 3.3.1. Применение различных асимметричных алгоритмов

В ОС Windows должны быть созданы две учетных записи: User1 и User2

1. Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с любым тестовым файлом с помощью стандартных средств ОС - EFS. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NFTS на том же компьютере, копировании папки на сетевой диск или диск с FAT.
2. Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.
3. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.
4. Зайдите в систему под встроенной учетной записью администратора и расшифруйте папку.

Результаты зафиксировать в отчете.

16. Задание к практическому занятию 3.3.2. Изучение программной реализации асимметричного алгоритма RSA

1. Реализовать программу для шифрования / дешифрования текстов, работающую по алгоритму RSA. Реализовать приложение для шифрования/ дешифрования, позволяющее вычислять открытый и закрытый ключи для алгоритма RSA:

1) числа p и q генерируются программой или задаются из файла;

2) числа p и q должны быть больше, чем 2128;

3) сгенерированные ключи сохраняются в файлы: открытый ключ – в один файл, закрытый – в другой.

4) исходный и зашифрованный тексты хранятся в файлах

2. Преподавателю демонстрируется работающая программа и предоставляется печатный отчёт. Отчёт содержит оформленный согласно требованиям код программы и несколько результатов работы программы. Необходимо объяснить принцип работы алгоритма при защите работы.

Результаты зафиксировать в отчете.

17. Задание к практическому занятию 3.4.1. Применение различных функций хеширования, анализ особенностей хешей

1. Реализовать приложение с графическим интерфейсом, позволяющее выполнять следующие действия.

1.1. Вычислять значение хэш-функции, заданной в варианте:

1) текст сообщения должен считываться из файла;

2) полученное значение хэш-функции должно представляться в шестнадцатеричном виде и сохраняться в файл;

3) при работе программы должна быть возможность просмотра и изменения считанного из файла сообщения и вычисленного значения хэш-функции.

1.2. Исследовать лавинный эффект на сообщении, состоящем из одного блока:

1) для бита, который будет изменяться, приложение должно позволять задавать его позицию (номер) в сообщении;

2) приложение должно уметь после каждого раунда (итерации цикла) вычисления хэш-функции подсчитывать число бит, изменившихся в хэше при изменении одного бита в тексте сообщения;

3) приложение может строить графики зависимости числа бит, изменившихся в хэше, от раунда вычисления хэш-функции, либо графики можно строить в стороннем ПО, но тогда приложение должно сохранять в файл необходимую для построения графиков информацию.

2. С помощью реализованного приложения выполнить следующие задания.

2.1. Протестировать правильность работы разработанного приложения.

2.2. Исследовать лавинный эффект при изменении одного бита в сообщении: для различных позиций изменяемого бита в сообщении построить графики зависимостей числа бит, изменившихся в хэше, от раунда вычисления хэш-функции (всего в отчѐте должно быть 2-3 графика).

2.3. Сделать выводы о проделанной работе.

Результаты зафиксировать в отчете.

18. Задание к практическому занятию 3.4.2. Применение криптографических атак на хеш-функции.

Проведение атаки перебором (bruteforce attack):

1. Используя программу для вскрытия паролей произвести атаку на зашифрованный файл. Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым;

2. Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

Проведение атаки по словарю (dictionary attack):

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, table, admin и т.д.). Провести атаку по словарю;

2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

Результаты зафиксировать в отчете.

19. Задание к практическому занятию 3.4.3. Изучение программно-аппаратных средств, реализующих основные функции ЭП

1. получите вариант задания у преподавателя;
2. сгенерируйте ЭЦП для сообщения;
3. проверьте подлинность ЭЦП для сообщения;
4. результаты и промежуточные вычисления оформите в виде отчета.

Результаты зафиксировать в отчете.

20. Задание к практическому занятию 3.5.1. Применение протокола ДиффиХеллмана для обмена ключами шифрования.

1. Изучить схему обмена ключами Диффи-Хелмана.
2. Реализовать подпрограмму, определяющую для заданного числа первые 100 первообразных корней, отображая при этом суммарное время, затраченное на их поиск. Число может задаваться десятеричной, шестнадцатеричной и двоичной формах.
3. Вручную для первых 5 полученных числовых значений привести доказательство, что они действительно являются первообразными корнями заданного числа n.
4. Реализовать подпрограмму, моделирующую обмен ключами между абонентами по схеме Диффи-Хеллмана. Программа должна получать большие простые числа XA, XB и n случайным образом с помощью алгоритма генерации простого числа, а также предоставлять пользователю возможность задавать их.

Результаты зафиксировать в отчете.

21. Задание к практическому занятию 3.5.2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

1. Проследите как происходит определение легальности клиента, логический вход в сеть, получение разрешения на продолжение процесса получения доступа к ресурсу через систему Kerberos.
2. Проследите как происходит получение разрешения на обращение к ресурсному серверу, например к файл серверу, серверу приложений, серверу удаленного доступа
3. Проследите как происходит получение разрешения на доступ к ресурсу. Изучите содержимое квитанции (билетов) на доступ к ресурсам.
4. Просмотрите системные журналы, логи на сервере Kerberos (на аутентификационной его части и на подсистеме, выдающей квитанции (билеты)), а также на ресурсных серверах.
5. Сделать выводы по работе и представить их в отчете.

Результаты зафиксировать в отчете.

22. Задание к практическому занятию 3.7.1. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей

1. Определить время перебора всех паролей, состоящих из 6 цифр. Алфавит составляют цифры n=10. Длина пароля 6 символов k=6.
2. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет. Алфавит составляют символы n=10.
3. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов. Длина пароля символов k. Скорость перебора s паролей в секунду. После каждого из m неправильно введенных паролей идет пауза в v секунд вариант n k s m v
4. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду. вариант n t s
5. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду. вариант k t s

Результаты зафиксировать в отчете.

23. Задание к практическому занятию 3.8.1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ

1. Изучить основные возможности ПО Filigrana
2. Изучить механизм встраивания ЦВЗ с использованием векторного квантования
3. Рассмотреть алгоритмы встраивания ЦВЗ с использованием скалярного квантования
4. Изучить алгоритмы на основе слияния ЦВЗ и контейнера
5. Изучить методы маскирования ЦВЗ

Результаты зафиксировать в отчете.

24. Задание к практическому занятию 3.8.2. Реализация простейших стеганографических алгоритмов

1. Изучить алгоритмов на основе линейного встраивания данных
2. Изучить принципы встраивания информации с использованием квантования. Дизеризованные квантователи.
3. Рассмотреть методы встраивания информации на уровне коэффициентов
4. Изучить методы встраивания информации на уровне битовой плоскости
5. Изучить метод встраивания информации за счет энергетической разности между коэффициентами

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Введение. Предмет и задачи криптографии. История криптографии. Основные термины.

1. Что такое шифрование?
1. способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
2. совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
3. удобная среда для вычисления конечного пользователя

2. Что такое кодирование?
1. преобразование обычного, понятного текста в код
2. преобразование
3. написание программы

3. Что является предметом науки криптография
1. способы шифрования и дешифрования
2. методы сокрытия факта передачи секретной информации
3. способы преобразования информации с целью ее защиты от несанкционированных пользователей

4. Первое известное применение шифра:
1. египетский текст
2. русский

3. нет правильного ответа

5. Выберите то, что относится к показателям криптостойкости:

1. количество всех возможных ключей
2. среднее время, необходимое для криптоанализа
3. количество символов в ключе

Раздел 1. Математические основы защиты информации

Тема 1.1. Математические основы криптографии

1. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

1. функцией Диффи-Хеллмана
2. односторонней функцией
3. функцией Эйлера
4. криптографической функцией

2. Какие из разделов математики легли в основу современных методов криптографии?

1. теория числе и абстрактная алгебра
2. теория кодирования и теория вероятности
3. теория сложности и теория дискретизации

3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

1. криптология
2. криптография
3. теория кодирования

4. В теоретической криптографии принято работать с алфавитом:

1. английским
2. любым национальным алфавитом
3. двоичных слов
4. 16-ричных слов

5. Какие виды математических последовательностей используются в криптографии:

1. детерминированные
2. случайные
3. неслучайные
4. бесконечные

Раздел 2. Классическая криптография

Тема 2.1. Методы криптографической защиты информации

1. Что представляет собой криптографическая система?

1. семейство T преобразований открытого текста, члены его семейства индексируются индексом k
2. программу
3. систему

2. Что принято называть электронной подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

3. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

4. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях? (выбрать все верные)

1. период порождаемой последовательности должен быть как можно меньше

2. вероятности порождения различных значений ключевой последовательности должны как можно больше отличаться друг от друга
3. период порождаемой последовательности должен быть очень большой
4. вероятности порождения различных значений ключевой последовательности должны быть равны

5. Криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот, называют:
1. симметричным;
2. ассиметричным;
3. синхронным;
4. асинхронным

Тема 2.2. Криптоанализ

1. Цель криптоанализа:
1. Определение стойкости алгоритма
2. Увеличение количества функций замещения в криптографическом алгоритме
3. Уменьшение количества функций подстановок в криптографическом алгоритме
4. Определение использованных перестановок

2. Криптоанализ предусматривает раскрытие секретных сообщений:
1. со знанием хотя бы одного из ключей
2. без знания криптографического алгоритма
3. без знания ключа и без знания криптографического алгоритма
4. без знания ключа, но со знанием криптографического алгоритма

3. Фундаментальное допущение криптоанализа, впервые сформулированное О. Кирхгоффом, состоит в том, что:
1. секретность сообщения полностью зависит от ключа
2. секретность сообщения полностью зависит от алгоритма шифрования
3. секретность сообщения зависит от ключа и алгоритма шифрования

4. Какие методы криптоанализа применяются для ассиметричных шифров?
1. DES
2. AES
3. RSA
4. COS

5. Какие методы криптоанализа применяются для симметричных шифров?
1. DES
2. AES
3. RSA
4. COS

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел

1. Поточный шифр выполняет преобразование входного сообщения:
1. блоками определенной длины
2. посимвольно

2. Для использования в криптографических целях генератор псевдослучайных чисел должен обладать следующими свойствами: (выбрать все верные)
1. период последовательности должен быть очень большой;
2. порождаемая последовательность должна быть "почти" случайной;
3. вероятности порождения различных значений должны быть в точности равны;
4. вероятности порождения различных значений должны быть различны

3. Какой из генераторов псевдослучайных чисел является наиболее простым?
1. Линейный конгруэнтный
2. Фибоначчи с запаздыванием
3. С квадратичным остатком (BBS)
4. На основе сдвиговых регистров с обратной связью

4. Какой алгоритм используется для шифрования паролей в ОС Windows, а также в протоколе SSL?

1. RC4
2. AES
3. TKIP

5. На чем основан принцип действия всех генераторов псевдослучайных чисел?

1. на физических явлениях или процессах, которые можно зафиксировать и сосчитать
2. на математических формулах

Раздел 3. Современная криптография

Тема 3.1. Кодирование информации. Компьютеризация шифрования.

1. Кодирование информации – это…

1. преобразование обычного, понятного текста в код
2. преобразование
3. написание программы

2. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

3. Какие коды используются в помехоустойчивом кодировании?

1. Хэмминга
2. CRC
3. БЧХ
4. Рида – Соломона
5. Грэя

4. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:

1. Оно обеспечивает проверку целостности и правильности данных
2. Оно требует внимательного отношения к процессу управления ключами
3. Оно не требует большого количества системных ресурсов
4. Оно требует передачи ключа на хранение третьей стороне (escrowed)

5. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

1. Коллизия
2. Хэширование
3. MAC
4. Кластеризация ключей

Тема 3.2. Симметричные системы шифрования

1. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

1. 1
2. 2
3. 3

2. Алгоритм, использующий симметричный ключ и алгоритм хэширования:

1. HMAC+
2. 3DES
3. ISAKMP-OAKLEY
4. RSA

3. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?

1. сложение по модулю 2
2. нахождение остатка от деления на большое простое число

3. замена бит по таблице замен
4. перестановка бит
5. возведение в степень

4. Какой размер ключа в отечественном стандарте симметричного шифрования:
1. 56 бит;
2. 124 бит;
3. 256 бит.

5. Что является преимуществом симметричного шифрования:
1. скорость выполнения криптографических преобразований;
2. легкость внесения изменений в алгоритм шифрования;
3. секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
4. применение в системах аутентификации (электронная подпись).

Тема 3.3. Асимметричные системы шифрования

1. Верны ли утверждения? (выбрать все верные)
1. В асимметричных криптосистемах не решена проблема распределения ключей.
2. Асимметричные криптосистемы существенно медленнее симметричных.

2. Асимметричные криптосистемы для шифрования информации используют количество ключей…. ?
1. 1
2. 2
3. 3
4. 4

3. В асимметричных системах шифрования
1. открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
2. для зашифрования и расшифрования используется один ключ
3. секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
4. секретный и открытый ключи доступны всем желающим

4. Какие шифры (механизмы обмена ключами) относятся к асимметричным (выбрать все верные):
1. Диффи–Хелмана (D-H)
2. Ривест–Шамир–Адлеман (RSA)
3. Криптография эллиптической кривой (ECC)

5. Какая связь существует между двумя ключами в асимметричной криптографии?
1. логическая
2. физическая
3. математическая
4. никакая

Тема 3.4. Аутентификация данных. Электронная подпись

1. Какие методы разрабатываются с целью обеспечения аутентификации?
1. методы подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия
2. методы присвоения уникального идентификатора взаимодействующим сторонам и самой информации в процессе информационного взаимодействия
3. оба ответа верны

2. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?
1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование

4. эффективное кодирование

3. Какая система является системой аутентификации и распределения ключей:

1. Kerberos
2. RSA
3. MD5
4. AES

4. Что принято называть электронной (цифровой) подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

5. Выберите то, что используют для создания цифровой подписи:

1. Закрытый ключ получателя
2. Открытый ключ отправителя
3. Закрытый ключ отправителя
4. Открытый ключ получателя

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

1. Позволяет ли обмениваться ключами по незащищенным каналам связи Метод Диффи-Хеллмана?

1. да
2. нет

2. Применяется ли для распределения ключей между пользователями информационной системы прямой обмен ключами между пользователями сети?

1. да
2. нет

3. Процесс согласования сессионного ключа в процессе информационного обмена называют _____ ключей.

1. распределением
2. идентификацией
3. аутентификацией
4. хэшированием

4. Какой протокол аутентификации является менее надежным?

1. PAP
2. CHAP

5. Сколько шагов предусматривает аутентификация с помощью протокола Kerberos версии 5 ?

1. 2
2. 3
3. 4
4. 5

Тема 3.6. Криптозащита информации в сетях передачи данных

1. Линейное шифрование это:

1. иптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
2. криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
3. несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2. Какой шифратор можно использовать для защиты передаваемой в Сеть информации?

1. обычный шифратор
2. проходной шифратор
3. табличный шифратор

3. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе по сети Интернет:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование

4. Какие из приведенных криптографических алгоритмов используют в основе сетей Фейстеля?

1. DES
2. Rijndael
3. оба ответа верны

5. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?

1. в системах предварительного распределения секретных ключей
2. в системах открытого распределения секретных ключей
3. оба ответа верны

Тема 3.7. Защита информации в электронных платежных системах

1. Механизмы защиты, которые как минимум должны быть реализованы для обеспечения функций защиты информации на отдельных узлах электронной платежной системы: выбрать все верные

1. обеспечение управления доступом на оконечных системах;
2. контролирование целостности и обеспечение конфиденциальности сообщения;
3. обеспечение взаимной аутентификации абонентов;
4. ведение регистрации и контролирование целостности последовательности сообщений
5. хранение персональной информации клиентов

2. Какой протокол передачи данных обеспечивает лучшую защиту в системах электронных платежей?

1. SSL
2. SET

3. Выберите все верные утверждения относительно протокола SSL:

1. Отсутствие аутентификации покупателя
2. Наличие аутентификации покупателя и продавца
3. Невозможность использования при операциях с банковским счетом
4. Открытость реквизитов покупателя при передаче по сети
5. Является на сегодняшний день самым безопасным для передачи платежных сообщений

4. В протоколе SET предусмотрены следующие типы ключей, используемых участниками платежных транзакций: выбрать все верные

1. ключ для подписи сообщения (Digital Signature Key);
2. ключ для шифрования данных (Data Encipherment Key);
3. ключ для подписи сертификата (Certificate Signature Key);
4. ключ для подписи списка отозванных сертификатов (CRL Signature Key).
5. ключ для дешифрования данных (Data Decryption Key);

5. Смарт-карта обеспечивает следующий набор функций: выбрать все верные

1. разграничение полномочий доступа к внутренним ресурсам;
2. шифрование данных с применением различных алгоритмов;
3. формирование электронной цифровой подписи;
4. выполнение всех операций взаимодействия владельца карты, банка и торговца.
5. создание безопасного сетевого канала для передачи платежных данных
6. дешифрование данных с применением различных алгоритмов

Тема 3.8. Компьютерная стеганография

1. Что может являться файлом – контейнером для стеганографии? выбрать все верные

1. файл изображения
2. файл звука
3. видеофайл
4. файл Word
5. файл Excel
6. исполняемые файлы

2. В стеганографии метод LSB это:
1. метод наименее значимого бита;
2. эхо-метод;
3. метод фазового кодирования;
4. метод расширенного спектра;

3. Какие принципы лежат в основе стеганографии? выбрать все верные
1. некоторые файлы могут быть искажены без потери их функциональности
2. неспособности человека различать незначительные искажения в графических или мультимедийных файлах
3. контрольная сумма и размер файла, несущего зашифрованную информацию не изменяется

4. Выберите верное утверждение:
1. стеганография скрывает тело сообщения
2. стеганография скрывает тело сообщения и факт его присутствия

5. Стеганографическая система или стегосистема – это:
1. совокупность средств и методов, которые используются для формирования скрытого канала передачи информации;
2. совокупность средств и методов, которые используются для маскировки ценной информации

5.2.1.3. УП.02.01. Учебная практика

Текущий контроль по учебной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:
1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:
- 90-100 баллов – при раскрытии всех разделов в полном объеме;
- 80-89 баллов – при раскрытии всех разделов с недочетами;
- 60-79 баллов – при раскрытии не всех разделов в полном объеме;
- 0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах

Задание 1. Изучите документацию к защищаемой автоматизированной системе и сформируйте перечень наиболее вероятных угроз для нее.

Задание 2. Сформируйте перечень программных и программно-аппаратных средств обеспечения информационной безопасности для защищаемой автоматизированной системы.

Задание 3. На основе проведенного анализа в заданиях 1 и 2, а также паспортов программных и программно-аппаратных средств обеспечения информационной безопасности предложите и обоснуйте выбор конкретных средств, наиболее подходящих в данных условиях и с учетом экономического фактора.

Задание 4. При наличии выбранных вами устройств выполните их монтаж (программную установку), настройку и проверьте их работу.

Тема 1.2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности.

Задание 1. Изучите инструкцию по диагностике, устранению отказов и обеспечению работоспособности программно-аппаратных средств обеспечения информационной безопасности для каждого конкретного средства.

Задание 2. Ознакомьтесь с приборами и инструментами, использующимися в диагностике, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности для каждого конкретного средства.

Задание 3. Используя приборы и инструменты, изученные в задании 2, выполните диагностику неполадки программно-аппаратного средства обеспечения информационной безопасности, а затем для выявленной неполадки предложите варианты ее устранения.

Задание 4. При наличии необходимых запчастей и материалов устраните неполадку и после ремонта проверьте качество работы программно-аппаратного средства обеспечения информационной безопасности.

Тема 1.3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.

Задание 1. Ознакомиться с инфраструктурой защищаемой информационной системы, а также с характеристиками применяемыми программно-аппаратными средствами обеспечения информационной безопасности.

Задание 2. С помощью теста сымитировать информационную атаку на защищаемую систему и оценить эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности.

Задание 3. Проанализировать результаты теста и при неудовлетворительных показателях предложить варианты их улучшения или замену программно-аппаратных средств, имеющих более высокую степень защиты.

Тема 1.4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации.

Задание 1. Изучить пути движения конфиденциальной информации в данном учреждении, составить схему.

Задание 2. Выполнить сортировку информации по критериям доступа, типу, способ обработки, хранения и передачи.

Задание 3. Составьте в Excel таблицу, в которой в строках будет перечислена дата и описание конфиденциальной информации, а в столбцах – критерии доступа, тип, способ обработки, хранения, передачи, источник, приемник. Как альтернативный вариант – таблица может быть составлена в виде БД в Access. Для безопасности рекомендуется защитить файл паролем.

Тема 1.5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации.

Задание 1. Изучить характер конфиденциальной информации и при наличии нескольких ее типов выполнить классификацию.

Задание 2. Изучить пути передачи информации, а также способ ее обработки.

Задание 3. На основе результатов, полученных в заданиях 1 и 2 выбрать ПО для обработки информации, которое может работать совместно с криптографической системой.

Задание 4. Настроить сетевую папку, доступ к которой возможен по логину и паролю и разместить в ней файлы с конфиденциальной информацией. Также настроить автоматическую архивацию файлов на сервере во избежание их потери.

Задание 5. С помощью межсетевого экрана на сервере заблокировать доступ к сетевой папке для всех несанкционированных пользователей учреждения.

Задание 6. На клиентских ПК настроить работу с файлами конфиденциальной информации в режиме шифрования либо подключить и настроить программу криптографии для передачи файлов по сети в зашифрованном виде.

Тема 1.6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.

Задание 1. Составить (а если уже составлена ранее, то ознакомиться) со схемой движения конфиденциальной информацией.

Задание 2. Классифицировать все элементы информационной системы предприятия по иерархическим уровням, к которым относятся не только компьютеры и сервера, но и помещения, ПО, математическое обеспечение и алгоритмы.

Задание 3. На основе стандартов и шаблонов составить (либо распечатать) бланки проверок для каждого элемента информационной системы, в которых будут указаны: аппаратное обеспечение, помещение, программное обеспечение, математическое обеспечение и алгоритмы, а также критерии проверки.

Задание 4. Составить схему маршрута обхода проверок по принципу «от низшей иерархии элементов ИС к высшей».

Тема 1.7. Устранение замечаний по результатам проверки.

Задание 1. Проанализировать на основе заполненных бланков проверок несоответствия и сформировать сводный лист исправлений замечаний по аттестации объектов, помещений, программ, алгоритмов.

Задание 2. Проанализировать каждое замечание и предложить варианты их устранения.

Задание 3. При наличии необходимых средств, деталей и материалов устранить выявленные замечания, после чего сделать отметку в листе исправлений с указание даты и подписи.

Тема 1.8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.

Задание 1. Изучить инструкции и рекомендации разработчика программно-аппаратных средств информационной безопасности.

Задание 2. Изучить инструкции и внутренние правила предприятия по обеспечению информационной безопасности программно-аппаратными средствами.

Задание 3. С помощью ГОСТов и справочно-правовых систем типа «Гарант» и «Консультант +» изучить нормативных правовых актов относительно обеспечения информационной безопасности программно-аппаратными средствами.

Задание 4. На основании документов, изученных в заданиях 1-3 скомпилировать проект внутреннего нормативного методического документа по обеспечению информационной безопасности программно-аппаратными средствами.

Тема 2.1. Применение математических методов для оценки качества и выбора наилучшего программного средства

Задание 1. Составить математическую модель, в которой в качестве целевой функции будет интегральный показатель защищенности информации, а в качестве параметров будут такие как: скорость работы системы по преобразованию информации, алгоритм криптографии, битовая длина ключа, вероятность взлома зашифрованного сообщения.

Задание 2. На основе математической модели составить на любом языке программу, в которую подставить значения параметров, соответствующие различным используемым криптографическим программным средствам.

Задание 3. Выполнить вычисления и по наибольшему показателю защищенности информации выбрать наилучшее криптографическое программное средство.

Тема 2.2. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.

Задание 1. Установить и настроить программу-криптопровайдер, например, Крипто-Про.

Задание 2. Установить и настроить необходимые плагины в веб-браузер для работы с информационной системой учреждения - контрагента.

Задание 3. С помощью специального ПО сгенерировать на флэш-носитель ключ электронной цифровой подписи (ЭЦП).

Задание 4. При необходимости установите и настройте программу для создания защищенного VPN-канала.

Задание 5. Установить корневой и личный сертификат ЭЦП в программу-криптопровайдер.

Задание 6. Проверить работу настроенной системы. Для этого войти с помощью браузера в информационную систему учреждения - контрагента под своей учетной записью, сформировать какой-либо документ, а затем подписать его с помощью личной ЭЦП (флэш-носитель должен быть вставлен в ПК) и отправить. На основании уведомлений сделать вывод о работоспособности настроенной системы защиты информации.

5.2.1.4. ПП.02.01. Производственная практика

Текущий контродь по производственной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

- 90-100 баллов – при раскрытии всех разделов в полном объеме;
- 80-89 баллов – при раскрытии всех разделов с недочетами;
- 60-79 баллов – при раскрытии не всех разделов в полном объеме;
- 0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Анализ принципов построения систем информационной защиты производственных подразделений

Задание 1. Изучите инфраструктуру комплекса АИС, АРМ, включая сетевую инфраструктуру.

Задание 2. Изучите требования и правила, действующие в производственных подразделениях с точки зрения информационной защиты.

Задание 3. Выпишите для себя наиболее «слабые места» с точки зрения информационной защиты и возможные угрозы.

Задание 4. Сформируйте перечень мероприятий для усиления наиболее «слабых мест» с точки зрения информационной защиты.

Тема 1.2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.

Задание 1. Ознакомьтесь с инструкцией по эксплуатации элементов программной защиты автоматизированной системы. Проверьте условия эксплуатации программной защиты – наличие конфликтующего ПО, установку всех необходимых обновлений ОС.

Задание 2. Ознакомьтесь с инструкцией по эксплуатации элементов аппаратной защиты автоматизированной системы. Проверьте условия эксплуатации аппаратной защиты – качество питающего напряжения, заземления, экранирования.

Задание 3. Проверьте исправность элементов охлаждения и отсутствия в них скоплений пыли, при необходимости произведите чистку и смазку вентиляторов.

Задание 4. Зафиксируйте в журнал выполненные работы.

Тема 1.3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.

Задание 1. Ознакомьтесь с инструкцией по эксплуатации элементов программной защиты автоматизированной системы. По заданию наставника проверьте наличие актуальных обновлений, при необходимости установите их. Проанализируйте системные журналы программных средств защиты на предмет ошибок.

Задание 2. Ознакомьтесь с инструкцией по эксплуатации элементов аппаратной защиты автоматизированной системы. По заданию наставника проверьте качество всех соединений. При наличии большого количества пыли выполните очистку оборудования.

Задание 3. Пронаблюдайте за действиями наставника по тестированию комплекса программно-аппаратных средств обеспечения информационной безопасности.

Задание 4. С помощью соответствующих приборов и инструментов проверьте качество питающей сети, заземления, а также надежность изоляции и экранирования.

Задание 5. При наличии замеченных дефектов в пунктах 1-4 зафиксируйте их и предложите способы их устранения.

Задание 6. После устранения выявленных дефектов под наблюдением наставника выполните повторное тестирование комплекса программно-аппаратных средств информационной защиты и сделайте соответствующую запись в журнале обслуживания.

Тема 1.4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении

Задание 1. Ознакомиться с типами и особенностями применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.

Задание 2. При наличии нескольких возможных или дублирующих средств защиты поочередно провести с каждым из них тестирование с имитацией информационных угроз. Записать все полученные результаты.

Задание 3. На основании полученных результатов сделать вывод об эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. Принять решение об использовании выбранного наиболее эффективного средства и отказе от наименее эффективных средств.

Тема 1.5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации

Задание 1. Ознакомиться с основными правилами учета, обработки, хранения и передачи конфиденциальной информации на примере определенного учреждения.

Задание 2. Проанализировать возможные угрозы информационной безопасности на каждом этапе этих процедур.

Задание 3. Сформировать и показать наставнику список возможных угроз, выполнить их классификацию по способам реализации и степени опасности, а также предложить варианты защиты от этих угроз.

Задание 4. После согласования угроз и методов защиты от них прослушать инструктаж, проводимый наставником для сотрудников учреждения.

Тема 1.6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.

Задание 1. Изучить нормативно-правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами, применяемыми в данном учреждении.

Задание 2. Изучить внутренние правила и инструкции учреждения по обеспечению информационной безопасности программно-аппаратными средствами.

Задание 3. Найти несоответствия между нормативными и внутренними документами, выяснить причину несоответствия и предложить варианты устранения этих несоответствий.

5.2.2. Оценочные средства при промежуточной аттестации

5.2.2.1. МДК.02.01. Программные и программно-аппаратные средства защиты информации

Формой промежуточной аттестации в седьмом сесместре является курсовой проект, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Курсовая работа(проект) является формой промежуточной аттестации обучающихся по дисциплине.

Курсовая работа(проект) выполняется обучающимися с целью:

1. формирования навыков применения теоретических знаний, полученных в ходе освоения дисциплины;
2. формирования практических навыков в части сбора, анализа и интерпретации результатов, необходимых для последующего выполнения научных научно-исследовательской работы;
3. формирования навыков логически и последовательно иллюстрировать подготовленную в процессе выполнения курсовой работы информацию;
4. формирования способностей устанавливать закономерности и тенденции развития явлений и процессов , анализировать , обобщать и формулировать выводы;
5. формировать умение использовать результаты, полученные в ход е выполнения курсовой работы в профессиональной деятельности.

Тема курсовой работы выбирается обучающимся самостоятельно

Примерные темы курсовых работ:

1. Цели и средства защиты информации. Типичный набор функциональных подсистем.
2. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности.
3. Понятие Защищенной системы обработки информации. Стандарты информационной безопасности и их роль.
4. Понятие угрозы безопасности компьютерной системы. Методы «взлома» компьютерных систем.
5. Защита компьютерной системы от «взлома». Программные закладки.
6. Методы уничтожения информации, хранимой на энергонезависимых носителях. Уровни степеней надежности.
7. Защита программного обеспечения. Превентивные меры защиты.
8. Защита программного обеспечения. Средства собственной защиты.
9. Защита программного обеспечения. Средства защиты в составе вычислительной системы.

10. Защита программного обеспечения. Средства защиты с запросом информации.
11. Защита программного обеспечения. Средства активной защиты.
12. Защита программного обеспечения. Средства пассивной защиты.
13. Технология защиты информации на основе: электронных ключей, смарт-карт, персональных идентификаторов.
14. Принципы и методы создания защищенной операционной системы.
15. Защита ресурсов ПЭВМ на аппаратном уровне.
16. Понятие замкнутой программной среды. Методология реализации. Мониторы безопасности объектов и субъектов.
17. Формирование и поддержка изолированной программной среды.
18. Политика безопасности защищенных компьютерных систем. Описательные категории.
19. Безопасное взаимодействие в КС.
20. Контроль и управление доступом.
21. Управление криптографическими ключами и хранение ключевой информации.
22. Концепция иерархии ключей. Распределение ключей.
23. Распределение ключей с участием центра распределения ключей. Протокол Kerberos.
24. СЗИ от НСД «Страж». Назначение, основные возможности.
25. СЗИ от НСД «DALLAS LOCK». Назначение, основные возможности.
26. СЗИ «SECRET NET». Назначение, основные возможности.
27. Программно-аппаратный комплекс СЗИ от НСД «АККОРД». Назначение, основные возможности.
28. Система защиты конфиденциальной информации «STRONGDISK». Назначение, основные возможности.
29. Система защиты корпоративной информации «SECRET DISK». Назначение, основные возможности.
30. Средство криптографической защиты информации «Верба». Назначение, основные возможности.
31. Средство криптографической защиты информации, криптопровайдер, «КриптоПРО». Назначение, основные возможности.
32. Комплексная система защиты информации «ПАНЦИРЬ». Назначение, основные возможности.
33. Система защиты информации от несанкционированного доступа «Аура». Назначение, основные возможности.
34. Аппаратно-программный модуль доверенной загрузки «КРИПТОН-ЗАМОК». Назначение, основные возможности.
35. СЗИ НСД «Блокпост». Назначение, основные возможности.
36. Система защиты информации «ЩИТ-РЖД». Назначение, основные возможности.
37. Система защиты информации ViPNet DISCguise. Назначение, основные возможности.
38. Система защиты информации ViPNet SafeDisk. Назначение, основные возможности.
39. Электронный замок «Соболь». Назначение, основные возможности.

Критерии оценивания курсовой работы:

90-100 баллов – исчерпывающее или достаточное изложение содержания тематики курсовой работы в пояснительной записке, соответствие структуры постельной записки курсовой работы установленным требованиям, уверенное изложение тематики курсовой работы в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

80-89 баллов – исчерпывающее но не достаточное изложение содержания тематики курсовой работы в пояснительной записке, незначительное не соответствие структуры постельной записки курсовой работы установленным требованиям, неуверенное изложение тематики курсовой работы в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

60–79 баллов – недостаточное изложение содержания тематики курсовой работы в пояснительной записке, нарушение структуры пояснительной записки курсовой работы

установленным требованиям, неуверенное изложение тематики курсовой работы в ходе процедуры защиты, верный ответ на один или отсутствие верных ответов на оба вопроса, или курсовая работа(проект) не представлена к проверке и защите.

0-59 баллов – курсовая работа(проект) не выполнена.

Количество баллов	0–59	60–79	80–89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Формой промежуточной аттестации в восьмом семестре является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Тестирование:

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопроса;
- 85...99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25...64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–74	75–84	85–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. Информация, полученная об информационной атаке может группироваться анализирующим сервером по следующим параметрам: (выбрать все верные)
   - IP-адресу атакующего;
   - порту получателя;
   - номеру агента;
   - дате, времени;
   - протоколу;
   - типу атаки
   - IP-адресу атакуемого
2. Протокольные системы обнаружения вторжений используются для….
   - Отслеживания трафика
   - Отслеживание вирусов
   - Отслеживание неисправностей
3. Что не включает архитектура системы обнаружения вторжений?
   - Хранилище
   - Сенсорную подсистему

- Оперативную память

4. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к…

- Хабу (коммутатору)
- Порту
- Мосту

5. Какого вида системы обнаружения вторжений не существует?

- Гибридная
- Цельная
- Узловая

6. Контроль защищенности информационной сети это:

- проверка документации по технике безопасности
- имитация "взлома" информационной сети, осуществляемая силами самой организации или уполномоченными лицами
- установка программно-аппаратных комплексов отслеживания попыток взлома сети
- установка камер видеонаблюдения по маршруту прохождения информационной сети

7. В какой политике безопасности для доступа к любому защищаемому объекту сети применимо запретительное правило: все, что не разрешено явно - запрещено.

- Политике безопасности по умолчанию
- Глобальной политика безопасности
- Стартовой политика безопасности
- Локальной политика безопасности

8. Межсетевой экран в защищенной информационной сети должен

- пропускать пакеты только в одну сторону
- обеспечивать безопасность внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи
- осуществлять контроль доступа пользователей внутренней сети
- полностью прекращать доступ между сетями

9. К системам анализа защищенности сети относится:

- Internet Scanner
- BS 7799
- Network IPS
- CRAMM

10. Механизмы защиты, реализованные в межсетевых экранах, серверах аутентификации, системах разграничения доступа, работают ___.

- только на этапе подготовки атаки
- только на этапе завершения атаки
- на всех этапах осуществления атаки
- только на этапе реализации атаки

Вариант 2.

1. При логическом группировании в виртуальных ЛКС используются такие процедуры управления пакетами, как ___ пакетов

- идентификация
- фильтрация
- сортировка

2. На каком уровне строятся наиболее распространенные VPN-системы:

- транспортном;
- прикладном;
- сетевом;
- канальном

3. В виртуальной частной сети реализуется топология:

- любая;

- точка-точка;
- шина;
- в виртуальной частной сети невозможно реализовать топологии.

4. С какой целью часто используются VPN типа «маршрутизатор—маршрутизатор»?

- Для предоставления заказчикам доступа к локальной сети компании.
- Для предоставления служащим доступа к сети компании из их дома.
- Для предоставления доступа к сети компании ее руководителям, находящимся в дороге.
- Для создания соединения между двумя офисами, расположенными на большом расстоянии друг от друга.

5. Аппаратные сети VPN на основе оборудования бывают (Выбрать все верные.):

- сети на основе маршрутизаторов
- сети на основе брандмауэров

6. Для подключения пользователей к сети компания использует беспроводные технологии. Были разработаны требования безопасности: Обеспечение конфиденциальной передачи данных; обеспечение целостности данных. Какие из перечисленных протоколов позволят решить поставленную задачу? (выбрать все верные):

- ESP
- WEP
- WPA
- 802.1x
- 802.11i

7. Политика безопасности компании запрещает пользователям посещение некоторых сайтов. Адреса сайтов занесены в черные списки, которые периодически обновляются. Кроме того, требуется блокировка любых баннеров. Какой из перечисленных типов брандмауэров позволит реализовать данную политику безопасности?

- Брандмауэр пакетной фильтрации
- NAT
- Брандмауэр уровня приложений
- RADIUS сервер
- PAT

8. В регистрационном журнале сервера обнаружены несколько подобных записей, свидетельствующих о реализации атаки: Jul 8 18:23:20 fender sshd[15019]: Illegal user bruce from 207.232.63.45

Какой тип систем обнаружения атак следует использовать для предотвращения вторжений такого типа в будущем?

- Анализаторы регистрационных файлов
- Анализаторы сетевой активности
- Мониторы регистрационных файлов
- Системы обнаружения атак на сетевом уровне
- Системы контроля целостности

9. Какой из перечисленных протоколов обеспечения сетевой безопасности является частью протокола IPSec и выполняет следующие функции: Обеспечение целостности данных; защита от повторения данных; удостоверение источника данных.

- AH
- MD5
- SNMP
- SSH
- ICV

10. Какой компонент защиты как минимум должен присутствовать в локальных и корпоративных сетях для обеспечения информационной безопасности:

- межсетевой экран

- механизм криптографии
- система обнаружения сетевых атак
- система обнаружения сетевых вторжений

Вариант 3.

1. Правила защиты информации – абстрактное описание комплекса программно-технических средств и организационных мер защиты от несанкционированного доступа к информации называется:
   - Модель
   - Макет
   - Прототип
   - Концепт
2. Укажите типовые методы изучения современных программно-аппаратных комплексов в условиях учебного заведения (выбрать все верные)
   - чтение инструкции, прилагаемой к программно-аппаратному комплексу
   - самостоятельное получение навыков в установке и настройке
   - проведение лабораторных работ
   - чтение форумов в Интернете
   - обращение в техподдержку
   - самостоятельное моделирование вариантов использования
3. Укажите типовые методы изучения современных программно-аппаратных комплексов в реальных рабочих условиях (выбрать все верные)
   - чтение инструкции, прилагаемой к программно-аппаратному комплексу
   - самостоятельное получение навыков в установке и настройке
   - чтение форумов в Интернете
   - обращение в техподдержку
   - самостоятельное моделирование вариантов использования
4. Наилучший эффект при изучении программно-аппаратного комплекса достигается при: (выбрать все верные)
   - самостоятельном изучении
   - наблюдении за специалистом, который имеет опыт в этом вопросе
   - обсуждении на форумах
   - обучении на специализированных курсах
   - все перечисленное
5. При изучении программно-аппаратного комплекса ответственность за его исправность и правильную работу возлагается на: (выбрать все верные)
   - производителя
   - специалиста, который его настраивает и вводит в эксплуатацию
   - специалиста, который будет его использовать
   - всех вышеперечисленных
6. Какая копия базы данных позволяет восстановить информацию полностью на 100% при сбое в любой момент времени?
   - Дифференциальная резервная копия
   - Резервная копия
   - Никакая из копий
7. Самым надежным способом защиты данных от потери является:
   - создание кластеров
   - резервное копирование данных и журнала транзакций
   - резервное копирование
   - технологии RAID
8. Верно ли утверждение: модель полного восстановления следует использовать для рабочей базы данных, содержащей критически важные данные?
   - да

- нет

9. Верно ли утверждение: простая модель восстановления может использоваться при разработке баз данных или при работе с базами, которые не требуют частого редактирования ?

- да
- нет

10. Виды защиты баз данных (выбрать все верные):

- защита всех учетных записей, защита идентифицированных объектов
- защита учётной записи группы администратора
- приложение, которое используется для управления базой данных
- защита группы Users
- дискреционная защита

Вариант 4.

1. Вредоносные программы – это ….

- шпионские программы
- программы, наносящие вред данным и программам, находящимся на компьютере
- антивирусные программы
- программы, наносящие вред пользователю, работающему на зараженном компьютере
- троянские утилиты и сетевые черви

2. К вредоносным программам относятся:

- Потенциально опасные программы
- Вирусы, черви, трояны
- Шпионские и рекламные программы
- Вирусы, программы-шутки, антивирусное программное обеспечение
- Межсетевой экран, брандмауэр.

3. Сетевые черви - это…

Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты, это:

- Вирусы, которые проникнув на компьютер, блокируют работу сети
- Вирусы, которые внедряются в документы под видом макросов
- Хакерские утилиты управляющие удаленным доступом компьютера
- Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей

4. Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...

- Загрузочный вирус;
- Макровирус;
- Троян;
- Сетевой червь;
- Файловый вирус.

5. Вирус поражающий документы называется

- Троян;
- Файловый вирус;
- Макровирус;
- Загрузочный вирус;
- Сетевой червь.

6. Какие основные меры защиты от НСК существуют: (выбрать все верные)

- Организационные
- Юридические
- Технические
- Компьютерные

7. Защита программ, установленных на жёстком диске реализуется в виде: (выбрать все верные):

- необходимость постоянно держать в накопителе носитель информации, например, компакт-диск или флэшку
- использование аппаратного USB или LPT – ключа
- привязка к серийным номерам компонентов компьютера
- сканирование локальной сети на предмет поиска подобной копии программы и блокирования ее
- проверка серийного номера программы через специальный сервер
- генерация уникального пароля при каждом запуске или копировании программы

8. Основные мотивы создания и использования систем защиты от копирования: (выбрать все верные)

- Учет условий распространения программных продуктов
- Учет возможностей пользователей программного продукта по снятию с него системы зашиты
- Учет свойств распространяемого программного продукта
- Оценка возможных потерь при снятии защиты и нелегальном использовании
- Постоянное обновление использованных в системе защиты средств
- Предоставление информации об объеме выпуска копий ПО в органы Госстата, налоговой инспекции
- Учет аппаратного обеспечения, на которое установлено ПО

9. Основные требования, предъявляемые к системе защиты от копирования: (выбрать все верные)

- обеспечение некопируемости дистрибутивных компакт-дисков стандартными средствами;
- обеспечение невозможности применения стандартных отладчиков без дополнительных действий над машинным кодом программы или без применения специализированных программно-аппаратных средств;
- обеспечение некорректного дизассемблирования машинного кода программы стандартными средствами;
- обеспечение сложности изучения алгоритма распознавания индивидуальных параметров компьютера, на котором установлен программный продукт, и его пользователя или анализа применяемых аппаратных средств защиты.
- ограничение на количество запусков программы (или обращений к папке, где установлена программа) в течение суток

10. Каких методов защиты информации от НСК не существует?

- методы, затрудняющие считывание скопированной информации;
- методы, препятствующие использованию информации
- методы, уничтожающие информацию (ПО) при использовании ее неавторизованным лицом

5.2.2.2. МДК.02.02. Криптографические средства защиты информации

Формой промежуточной аттестации в шестом сесместре является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к экзамену:

1. Предмет криптографии. Определения. Задачи. Исторические примеры.
2. Виды атак на криптографические алгоритмы. Понятие стойкости.
3. Классификация алгоритмов шифрования. Примеры простейших шифров.
4. Шифры замены. Математическая модель. Примеры.
5. Шифры перестановки. Математическая модель. Примеры.
6. Шифры гаммирования. Математическая модель. Примеры.
7. Принципы построения блочных шифров. Схема Фейстеля.
8. Алгоритм симметричного шифрования DES.
9. Алгоритм симметричного шифрования ГОСТ 28147-99.
10. Алгоритм симметричного шифрования Rijndael.
11. Алгоритмы симметричного шифрования IDEA и Blowfish.
12. Режимы выполнения алгоритмов симметричного шифрования.
13. Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
14. Линейные конгруэнтные генераторы. Линейные регистры сдвига.
15. Поточные шифры. Отличия от блочных. Стойкость. Методы анализа.
16. Примеры поточных шифров на основе LFSR.
17. Примеры поточных шифров, использующих аддитивные генераторы.
18. Примеры поточных шифров на основе FCSR.
19. Математические методы криптоанализа: метод опробывания, методы на основе теории статистических решений.
20. Линейный криптоанализ.
21. Разностный криптоанализ.
22. Основные принципы построения асимметричных криптосистем. Стойкость.
23. Шифросистема RSA. Стойкость.
24. Шифросистема Эль-Гамаля. Стойкость.
25. Шифросистема на основе принципа «рюкзака».
26. Шифросистема Рабина. Стойкость.
27. Алгоритм обмена ключами Диффи-Хеллмана.
28. Хэш-функции. Требования. Типы функций хэширования.
29. Атаки на функции хэширования.
30. Функция хеширования MD5.
31. Функция хеширования SHA-1.
32. Функция хеширования ГОСТ 3411-94.
33. Функция хеширования СТБ 1176.1-99.
34. Общие положения электронной цифровой подписи. Задачи. Требования.
35. Прямая и арбитражная цифровая подписи. Примеры.

36. Стандарт электронной цифровой подписи DSS.
37. Цифровая подпись на основе алгоритмов с открытыми ключами. Схема Фиата-Шамира.
38. Цифровая подпись Эль-Гамаля. Схема RSA.
39. Стандарт электронной цифровой подписи DSS.
40. Стандарт электронной цифровой подписи ГОСТ-Р 34.10-94.
41. Стандарт электронной цифровой подписи СТБ 1176.2-99.
42. Применение эллиптических кривых в криптографии. Алгоритм шифрования на основе эллиптических кривых.
43. Алгоритмы обмена ключами и электронной цифровой подписи на основе эллиптических кривых.
44. Стеганографические методы защиты информации. Основные понятия и определения. Области применения.
45. Общая модель стеганосистемы. Проблема устойчивости. Стегоанализ.
46. Методы сокрытия информации в неподвижных изображениях.
47. Методы сокрытия информации в текстовых данных.
48. Протоколы аутентификации. Двусторонняя аутентификация.
49. Протоколы аутентификации. Односторонняя аутентификация.

Тестирование:

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопроса;
- 85...99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25...64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–74	75–84	85–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. Линейное шифрование это:

1. иптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
2. криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
3. несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2. Какие из приведенных криптографических алгоритмов используют в основе сетей Фейстеля?

1. DES
2. Rijndael
3. оба ответа верны

3. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?

1. в системах предварительного распределения секретных ключей
2. в системах открытого распределения секретных ключей
3. оба ответа верны

4. Позволяет ли обмениваться ключами по незащищенным каналам связи Метод Диффи-Хеллмана?

1. да

2. нет

5. Какой протокол аутентификации является менее надежным?

1. PAP
2. CHAP

6. Сколько шагов предусматривает аутентификация с помощью протокола Kerberos версии 5 ?

1. 2
2. 3
3. 4
4. 5

7. Для использования в криптографических целях генератор псевдослучайных чисел должен обладать следующими свойствами: (выбрать все верные)

1. период последовательности должен быть очень большой;
2. порождаемая последовательность должна быть "почти" случайной;
3. вероятности порождения различных значений должны быть в точности равны;
4. вероятности порождения различных значений должны быть различны

8. Какой из генераторов псевдослучайных чисел является наиболее простым?

1. Линейный конгруэнтный
2. Фибоначчи с запаздыванием
3. С квадратичным остатком (BBS)
4. На основе сдвиговых регистров с обратной связью

9. Какой алгоритм используется для шифрования паролей в ОС Windows, а также в протоколе SSL?

1. RC4
2. AES
3. TKIP

10. На чем основан принцип действия всех генераторов псевдослучайных чисел?

1. на физических явлениях или процессах, которые можно зафиксировать и сосчитать
2. на математических формулах

Вариант 2.

1. Механизмы защиты, которые как минимум должны быть реализованы для обеспечения функций защиты информации на отдельных узлах электронной платежной системы: выбрать все верные

1. обеспечение управления доступом на оконечных системах;
2. контролирование целостности и обеспечение конфиденциальности сообщения;
3. обеспечение взаимной аутентификации абонентов;
4. ведение регистрации и контролирование целостности последовательности сообщений
5. хранение персональной информации клиентов

2. В протоколе SET предусмотрены следующие типы ключей, используемых участниками платежных транзакций: выбрать все верные

1. ключ для подписи сообщения (Digital Signature Key);
2. ключ для шифрования данных (Data Encipherment Key);
3. ключ для подписи сертификата (Certificate Signature Key);
4. ключ для подписи списка отозванных сертификатов (CRL Signature Key).
5. ключ для дешифрования данных (Data Decryption Key);

3. Смарт-карта обеспечивает следующий набор функций: выбрать все верные

1. разграничение полномочий доступа к внутренним ресурсам;
2. шифрование данных с применением различных алгоритмов;
3. формирование электронной цифровой подписи;
4. выполнение всех операций взаимодействия владельца карты, банка и торговца.
5. создание безопасного сетевого канала для передачи платежных данных
6. дешифрование данных с применением различных алгоритмов

4. Какая система является системой аутентификации и распределения ключей:

1. Kerberos
2. RSA
3. MD5
4. AES

5. Что принято называть электронной (цифровой) подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

6. Выберите то, что используют для создания цифровой подписи:

1. Закрытый ключ получателя
2. Открытый ключ отправителя
3. Закрытый ключ отправителя
4. Открытый ключ получателя

7. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

8. Какие коды используются в помехоустойчивом кодировании?

1. Хэмминга
2. CRC
3. БЧХ
4. Рида – Соломона
5. Грэя

9. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:

1. Оно обеспечивает проверку целостности и правильности данных
2. Оно требует внимательного отношения к процессу управления ключами
3. Оно не требует большого количества системных ресурсов
4. Оно требует передачи ключа на хранение третьей стороне (escrowed)

10. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

1. Коллизия
2. Хэширование
3. MAC
4. Кластеризация ключей

Вариант 3.

1. Какие принципы лежат в основе стеганографии? выбрать все верные

1. некоторые файлы могут быть искажены без потери их функциональности
2. неспособности человека различать незначительные искажения в графических или мультимедийных файлах
3. контрольная сумма и размер файла, несущего зашифрованную информацию не изменяется

2. Выберите верное утверждение:

1. стеганография скрывает тело сообщения
2. стеганография скрывает тело сообщения и факт его присутствия

3. Стеганографическая система или стегосистема – это:

1. совокупность средств и методов, которые используются для формирования скрытого канала передачи информации;
2. совокупность средств и методов, которые используются для маскировки ценной информации

4. В асимметричных системах шифрования

1. открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
2. для зашифрования и расшифрования используется один ключ
3. секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
4. секретный и открытый ключи доступны всем желающим

5. Какие шифры (механизмы обмена ключами) относятся к асимметричным (выбрать все верные):

1. Диффи–Хелмана (D-H)
2. Ривест–Шамир–Адлеман (RSA)
3. Криптография эллиптической кривой (ECC)

6. Какая связь существует между двумя ключами в асимметричной криптографии?

1. логическая
2. физическая
3. математическая
4. никакая

7. Алгоритм, использующий симметричный ключ и алгоритм хэширования:

1. HMAC+
2. 3DES
3. ISAKMP-OAKLEY
4. RSA

8. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?

1. сложение по модулю 2
2. нахождение остатка от деления на большое простое число
3. замена бит по таблице замен
4. перестановка бит
5. возведение в степень

9. Какой размер ключа в отечественном стандарте симметричного шифрования:

1. 56 бит;
2. 124 бит;
3. 256 бит.

10. Что является преимуществом симметричного шифрования:

1. скорость выполнения криптографических преобразований;
2. легкость внесения изменений в алгоритм шифрования;
3. секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
4. применение в системах аутентификации (электронная подпись).

Вариант 4.

1. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

1. функцией Диффи-Хеллмана
2. односторонней функцией
3. функцией Эйлера
4. криптографической функцией

2. Какие из разделом математики легли в основу современных методов криптографии?

1. теория числе и абстрактная алгебра
2. теория кодирования и теория вероятности
3. теория сложности и теория дискретизации

3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

1. криптология
2. криптография
3. теория кодирования

4. В теоретической криптографии принято работать с алфавитом:

1. английским
2. любым национальным алфавитом
3. двоичных слов
4. 16-ричных слов

5. Какие виды математических последовательностей используются в криптографии:

1. детерминированные
2. случайные
3. неслучайные
4. бесконечные

6. Что представляет собой криптографическая система?

1. семейство T преобразований открытого текста, члены его семейства индексируются индексом k
2. программу
3. систему

7. Что принято называть электронной подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

8. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

9. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях? (выбрать все верные)

1. период порождаемой последовательности должен быть как можно меньше
2. вероятности порождения различных значений ключевой последовательности должны как можно больше отличаться друг от друга
3. период порождаемой последовательности должен быть очень большой
4. вероятности порождения различных значений ключевой последовательности должны быть равны

10. Криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот, называют:

1. симметричным;
2. ассиметричным;
3. синхронным;
4. асинхронным

Вариант 5.

1. Что представляет собой криптографическая система?

1. семейство T преобразований открытого текста, члены его семейства индексируются индексом k
2. программу
3. систему

2. Что принято называть электронной подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

3. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

4. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях? (выбрать все верные)

1. период порождаемой последовательности должен быть как можно меньше
2. вероятности порождения различных значений ключевой последовательности должны как можно больше отличаться друг от друга
3. период порождаемой последовательности должен быть очень большой
4. вероятности порождения различных значений ключевой последовательности должны быть равны

5. Криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот, называют:

1. симметричным;
2. ассиметричным;
3. синхронным;
4. асинхронным

6. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

1. функцией Диффи-Хеллмана
2. односторонней функцией
3. функцией Эйлера
4. криптографической функцией

7. Какие из разделов математики легли в основу современных методов криптографии?

1. теория числе и абстрактная алгебра
2. теория кодирования и теория вероятности
3. теория сложности и теория дискретизации

8. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

1. криптология
2. криптография
3. теория кодирования

9. В теоретической криптографии принято работать с алфавитом:

1. английским
2. любым национальным алфавитом
3. двоичных слов
4. 16-ричных слов

10. Какие виды математических последовательностей используются в криптографии:

1. детерминированные
2. случайные
3. неслучайные
4. бесконечные

Вариант 3.6

1. Кодирование информации – это…

1. преобразование обычного, понятного текста в код
2. преобразование
3. написание программы

2. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые

2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

3. В чем заключается общая идея помехоустойчивого кодирования?
1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

4. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:
1. Оно обеспечивает проверку целостности и правильности данных
2. Оно требует внимательного отношения к процессу управления ключами
3. Оно не требует большого количества системных ресурсов
4. Оно требует передачи ключа на хранение третьей стороне (escrowed)

5. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:
1. Коллизия
2. Хэширование
3. MAC
4. Кластеризация ключей

6. Цель криптоанализа:
1. Определение стойкости алгоритма
2. Увеличение количества функций замещения в криптографическом алгоритме
3. Уменьшение количества функций подстановок в криптографическом алгоритме
4. Определение использованных перестановок

7. Криптоанализ предусматривает раскрытие секретных сообщений:
1. со знанием хотя бы одного из ключей
2. без знания криптографического алгоритма
3. без знания ключа и без знания криптографического алгоритма
4. без знания ключа, но со знанием криптографического алгоритма

8. Фундаментальное допущение криптоанализа, впервые сформулированное О. Кирхгоффом, состоит в том, что:
1. секретность сообщения полностью зависит от ключа
2. секретность сообщения полностью зависит от алгоритма шифрования
3. секретность сообщения зависит от ключа и алгоритма шифрования

9. Какие методы криптоанализа применяются для ассиметричных шифров?
1. DES
2. AES
3. RSA
4. COS

10. Какие методы криптоанализа применяются для симметричных шифров?
1. DES
2. AES
3. RSA
4. COS

5.2.2.3 УП.02.01. Учебная практика

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Установка программного обеспечения в соответствии с технической документацией.

1. Приведите пример наиболее известных программных средств обеспечения информационной безопасности в автоматизированных системах.
2. Приведите пример наиболее известных программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах
3. Приведите пример по ограничению в применении какого-либо программного и программно-аппаратного средства обеспечения информационной безопасности в автоматизированных системах
4. Какие параметры являются критерием применимости программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах?
5. Как, чем и кем оценивается правильность применения программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах?

Тема 1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.

1. Какие типы отказов существуют в программно-аппаратных средствах обеспечения информационной безопасности?
2. Каким образом производится устранение отказов в программно-аппаратных средствах обеспечения информационной безопасности?
3. Какие инструменты и средства используются при диагностике программно-аппаратных средств обеспечения информационной безопасности?
4. Какие мероприятия способствуют обеспечению работоспособности программно-аппаратных средств обеспечения информационной безопасности?
5. Существуют ли какие-либо нормы времени на устранение отказов программно-аппаратных средств обеспечения информационной безопасности?

Тема 1.3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности.

1. На основе каких критериев делается оценка об эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?
2. Какие методики или тесты используются при оценке эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?
3. Кто уполномочен делать оценку эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?
4. Что делать в случае неудовлетворительной оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности?
5. Существует ли какая-то интегральная шкала оценок эффективности? Если да, то как она выглядит?

Тема 1.4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации

1. Как выглядит типовая схема путей движения конфиденциальной информации в большинстве учреждении?
2. В каком виде составляется документация по учету, обработке, хранению и передаче конфиденциальной информации?
3. Кем составляется документация по учету, обработке, хранению и передаче конфиденциальной информации?
4. Используются ли какие-либо принципы автоматизации при составлении документации по учету, обработке, хранению и передаче конфиденциальной информации? Если да, то приведите пример.
5. Для чего составляется документация по учету, обработке, хранению и передаче конфиденциальной информации?

Тема 1.5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации

1. Существует ли какое-либо специализированное ПО для обработки, хранения и передачи конфиденциальной информации? Если да, то приведите пример.
2. Какие используются стандартные программные средства при обработке, хранении и передаче конфиденциальной информации?
3. Какие средства защиты конфиденциальной информации используются для передачи между двумя клиентскими ПК? Приведите пример.
4. Какие существуют встроенные в ОС Windows средства защиты конфиденциальных файлов при работе в сетевой среде?
5. Какие существуют средства защиты для хранения конфиденциальной информации на серверах?

Тема 1.6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.

1. Какие сведения нужны для составления маршрута при проведении различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов?
2. Что представляет собой маршрут для проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов? В каком виде он может быть представлен?
3. Какие элементы информационной системы относятся к низшей иерархии, а какие к высшей?
4. Где можно взять или как составить бланки для проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов? В каком виде могут существовать эти бланки?
5. Существует ли какое-либо специальное ПО для составления маршрута проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов?

Тема 1.7. Устранение замечаний по результатам проверки.

1. Как выглядит и в какой форме может быть представлен сводный лист исправлений замечаний по аттестации объектов, помещений, программ, алгоритмов?
2. Какие замечания являются существенными, а какие несущественными? Приведите пример.
3. Что требуется для устранения замечаний?
4. Существуют ли какие-либо временные нормативы для устранения замечаний?
5. Кто уполномочен устранять замечания по результатам проверки?

Тема 1.8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов

1. Кто разрабатывает и утверждает внутренние нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами в учреждении?

2. Кто разрабатывает и утверждает федеральные нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами?

3. Как связаны и как соотносятся между собой внутренние и федеральные нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами с инструкциями от разработчика этих средств?

4. При составлении (компиляции) внутреннего нормативного методического документа по обеспечению информационной безопасности программно-аппаратными средствами из инструкций разработчика, федеральных документов, внутренних документов предприятия в каком порядке расставляются приоритеты?

5. Кем рассматриваются и утверждаются проекты внутренних нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами на предприятии?

Тема 2.1. Применение математических методов для оценки качества и выбора наилучшего программного средства

1. Приведите пример математической модели для оценки качества и выбора наилучшего программного средства? Что можно использовать в качестве целевой функции, а что в качестве параметров?

2. Можно ли с помощью Excel реализовать какую-либо математическую модель, оценить качество и сделать выбор наилучшего программного средства?

3. Что представляет собой интегральный показатель защищенности информации? Из чего он состоит?

4. Что является критерием качества ПО для защиты информации?

5. Существуют ли готовые математические формулы для оценки качества и выбора наилучшего программного средства защиты информации? Если да, то приведите пример.

Тема 2.2. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи.

1. Что такое программа-криптопровайдер и для чего она нужна? приведите примеры.

2. Какие плагины необходимо чаще всего подключить к веб-браузеру, чтобы работать, например, с казначейством, налоговой инспекцией, банком, пенсионным фондом?

3. Кратко опишите процесс генерации ключей к электронной цифровой подписи (ЭЦП). Кем генерируются ключи?

4. Для чего нужны корневой и личный сертификат, устанавливаемый на рабочее место сотрудника, работающего с информационной системой?

5. Существуют ли особые требования к хранению и использованию ключевых носителей ЭЦП? Если да, то какие именно?

5.2.2.4 ПП.02.01. Производственная практика

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Анализ принципов построения систем информационной защиты производственных подразделений.

1. Что относится к инфраструктуре комплекса АИС, АРМ?

2. Какие вы знаете системы информационной защиты, использующиеся в производственных подразделениях?

3. Что понимается под принципами построения систем информационной защиты производственных подразделений?

4. Сформулируйте кратко основные принципы построения систем информационной защиты производственных подразделений.

5. На основе каких критериев можно выполнить анализ принципов построения систем информационной защиты производственных подразделений и сделать вывод об их эффективности?

Тема 1.2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.

1. Что относится к условиям эксплуатации элементов программной защиты автоматизированной системы?

2. Что относится к условиям технической эксплуатации элементов аппаратной защиты автоматизированной системы?

3. Какие аппаратные элементы системы защиты нуждаются в периодическом обслуживании?

4. Возможна ли эксплуатация элементов программной и аппаратной защиты автоматизированной системы при несоответствии какого-либо параметра? И если да, то при каких условиях?

5. Существуют ли какие-либо определенные сроки эксплуатации элементов программной и аппаратной защиты автоматизированной системы?

Тема 1.3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности.

1. Какие ошибки в работе программно-аппаратных средств обеспечения информационной безопасности указываются в системном журнале?

2. Нужна ли какая-то группа допуска или особое разрешение при выполнении таких работ, как например, удаление пыли из аппаратных элементов средств обеспечения информационной безопасности?

3. Что представляют собой тесты и процедура тестирования комплекса программно-аппаратных средств обеспечения информационной безопасности?

4. Какие приборы и инструменты используются при оценке качества питающей сети, заземления, а также надежности изоляции и экранирования?

5. Какие можно делать выводы на основании записей в журнале обслуживания программно-аппаратных средств обеспечения информационной безопасности?

Тема 1.4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении.

1. Как и с помощью чего производится тестирование с имитацией информационных угроз?

2. Как классифицируются типы применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении?

3. Какие критерии используются для оценки эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении?

4. Чем следует руководствоваться при принятии решения по выбору используемого программно-аппаратного средства обеспечения информационной безопасности в структурном подразделении?

5. В каком виде для руководства предприятия удобнее представить результаты анализа эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении?

Тема 1.5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации.

1. На что следует обратить внимание при изучении правил учета, обработки, хранения и передачи конфиденциальной информации на примере определенного учреждения?

2. Какие возможны виды угроз в процессах учета, обработки, хранения и передачи конфиденциальной информации?

3. Какие мероприятия могут снизить вероятность угроз в процессах учета, обработки, хранения и передачи конфиденциальной информации?

4. Какими основными принципами следует руководствоваться при разработке (либо модернизации) правил учета, обработки, хранения и передачи конфиденциальной информации?

5. Какие основные требования предъявляются к системе учета и мониторинга процессов обработки, хранения и передачи конфиденциальной информации?

Тема 1.6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики

1. Какие существуют нормативно-правовые акты по обеспечению информационной безопасности программно-аппаратными средствами?

2. Какие существуют нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами?

3. Кто разрабатывает локальные нормативные документы по обеспечению информационной безопасности программно-аппаратными средствами на данном предприятии?

4. Кто контролирует исполнение правил по обеспечению информационной безопасности программно-аппаратными средствами на данном предприятии?

5. Если имеются некоторые противоречия между государственными и локальными нормативными документами по обеспечению информационной безопасности программно-аппаратными средствами на данном предприятии, то какие документы имеют приоритет?

5.2.3. Экзамен по модулю

Промежуточная аттестация по профессиональному модулю ПМ 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами проходит в виде экзамена.

Условия подготовки и процедура проведения экзамена

Преподаватели профессионального цикла разрабатывают контрольно-оценочные средства для проведения комплексной оценки сформированности профессиональных для промежуточной аттестации по профессиональному модулю, перечень наглядных пособий, материалов справочного характера, нормативных документов и различных образцов, которые разрешены к использованию на экзамене.

К экзамену допускаются обучающиеся, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по профессиональному модулю.

5.2.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этап формирования компетенций

На экзамен все обучающиеся приходят в соответствии с расписанием, в установленное время. Каждому студенту выдается билет, в котором имеются четыре вопроса и лист бумаги. На лист бумаги студент записывает ФИО, номер билета и содержащиеся в нем вопросы. Время для ответа на вопросы 35-45 минут. Ответы даются в письменном виде. По истечении указанного времени листы с ответами сдаются преподавателю. Результаты оценивания ответов на вопросы доводятся до сведения обучающихся в тот же день. Если студент воспользовался внешним источником информации, его ответы не принимаются, и выставляется неудовлетворительная оценка.