МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ ДАГЕСТАН

«КИЗЛЯРСКИЙ ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

ФОНД ОЦЕНОЧНЫХСРЕДСТВ
ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

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

код и название по ФГОС

10.02.05 Обеспечение информационной безопасности автоматизированных систем

код и наименование специальности

Кизляр, 2024г.

Фонд оценочных средств профессионального модуля ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» составлен на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО)

10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Приказом Министерства образования и науки от 09.12.2016 № 1553. Фонд оценочных средств соответствует требованиям к содержанию, структуре, оформлению.

Организация – разработчик: Организация-разработчик: ГБПОУ РД «Кизлярский профессионально-педагогический колледж».

Разработчик: Заманов Б.Х., преподаватель профессиональных дисциплин

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

Перечень видов оценочных средств соответствует Рабочей программе профессионального модуля.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме тестовых заданий и промежуточной аттестации в форме тестовых заданий и практических заданий.

Структура и содержание заданий – задания разработаны в соответствии с рабочей программой ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Освоение содержания ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами обеспечивает достижение студентами следующих **результатов**:

Таблица 1 Перечень общих компетенций и личностных результатов:

Код	Наименование общих компетенций
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.
ЛР 13	Поддерживающий коллективизм и товарищество в организации инженерной деятельности, развитие профессионального и общечеловеческого общения, обеспечение разумной свободы обмена научно-технической информацией, опытом.
ЛР 16	Стремящийся к постоянному повышению профессиональной квалификации, обогащению знаний, приобретению профессиональных умений и компетенций, овладению современной компьютерной культурой, как необходимому условию освоения новейших методов познания, проектирования, разработки экономически грамотных, научно обоснованных технических решений, организации труда и управления, повышению общей культуры поведения и общения.
ЛР 17	Борющийся с невежеством, некомпетентностью, технофобией, повышающий свою техническую культуру.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
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.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	− установки, настройки программных средств защиты информации в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностика, устранения отказов и восстановления 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.
Уметь	− 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; − 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 средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
Знать	– 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; – 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 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.

ФОРМЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ ЭЛЕМЕНТОВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Элемент модуля	Форма контроля и оценивания		
	Промежуточная аттестация	**Рубежный контроль**	**Текущий контроль**
МДК.02.01. Программные и программно-аппаратные средства защиты информации	Дифференцированный зачет (6 семестр), Курсовая работа (7 семестр), Экзамен (7 семестр)	Контрольная работ	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Тестирование; Контроль выполнения самостоятельной работы;
МДК.02.02 Криптографические средства защиты информации	Дифференцированный зачет (6 семестр)	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы;	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Контроль выполнения самостоятельной работы; Оценка результатов выполнения контрольных работ; Защита курсовой работы (курсового проекта);
УП. 02	Дифференцированный зачет (7 семестры)	------	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП 02	Дифференцированный зачет (8 семестр)	------	Оценка выполнения работ и оформления отчетной документации на производственной практике
Профессиональный модуль ПМ.02	Экзамен по модулю		

3. ФОРМЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ ЭЛЕМЕНТОВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

В результате текущей аттестации по ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

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

Элемент учебной дисциплины	**Формы и методы контроля**					
	Текущий контроль		**Рубежный контроль**			
	Форма контроля	**Проверяемые ОК, У, З**	**Форма контроля**	**Проверяемые ОК, У, З**	**Форма контроля**	**Проверяемые ОК, У, З**
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Устный опрос	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У		
Тема 1.2. Защищенная автоматизированная система	Устный опрос. Практические работы № 1-4	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		

Тема 1.3. Дестабилизирующее воздействие на объекты защиты	Устный опрос. Практические работы № 5	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Практические работы № 12	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		
Тема 1.4. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Устный опрос. Практическая работа № 6	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 1.5. Защита программ от изучения	Устный опрос.	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З

Тема 1.6. Вредоносное программное обеспечение	Устный опрос Практические работы № 7-8	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 1.7. Защита информации на машинных носителях	Устный опрос Практические работы № 9-10	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 1.8. Системы обнаружения атак и вторжений	Устный опрос. Практическая работа № 11	ОК 08 ПК 2.1 ПК 2.2		ОК 08 ПК 2.1 ПК 2.2	Экзамен	ОК 08 ПК 2.1 ПК 2.2
		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6

		У З		У З		У З
Тема 1.9. Средства организаци и VPN	Устный опрос. Практические работы № 12	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 1.10. Обеспечение безопасности межсетевого взаимодействия	Устный опрос. Практические работы № 13-14	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Практические работы № 22	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 1.11. Защита информации в базах данных	Устный опрос Практические работы № 15	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5

		ПК 2.6 У З		ПК 2.6 У З		ПК 2.6 У З
Тема 1.12. Мониторинг систем защиты	Устный опрос. Практическая работа № 16	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3
		ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 1.13. Изучение современных программно-аппаратных комплексов.	Устный опрос Практическая работа № 17-20	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У		ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У	Экзамен	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У

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

Элемент учебной дисциплины	Формы и методы контроля					
	Текущий контроль		Рубежный контроль		Промежуточная аттестация	
	Форма контроля	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З	Форма контроля	Проверяемые ОК, У, З
Тема 1.1. Математические основы криптографии	Устный опрос. Практические работы № 1-6	ОК 08 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 2.1. Методы криптографического защиты информации	Устный опрос. Практические работы № 7-9	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	Контрольная работа № 1	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З

Тема 2.2. Криптоанализ	Устный опрос. Практические работы № 10-12	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 2.3. Поточные шифры и	Устный опрос. Практическая работа № 13-14	ОК 01-ОК 10 ПК 2.1		ОК 01-ОК 10 ПК 2.1	экзамен	ОК 01-ОК 10 ПК 2.1
генераторы псевдослучайных чисел		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 3.1. Кодирование информации. Компьютеризация шифрования	Устный опрос. Практические работы № 15-18	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6

		У З		У З		У З
Тема 3.2. Симметричные системы шифрования	Устный опрос. Практическая работа № 19	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 3.3. Асимметричные системы шифрования	Устный опрос. Практические работы № 20	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 3.4. Алгоритмы обмена ключей и	Устный опрос. Практические работы № 21	ОК 01-ОК 10 ПК 2.1 ПК 2.2	Практические работы № 55	ОК 01-ОК 10 ПК 2.1 ПК 2.2	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2
протоколы аутентификации		ПК 2.3 ПК 2.4		ПК 2.3 ПК 2.4		ПК 2.3 ПК 2.4

		ПК 2.5 ПК 2.6 У З		ПК 2.5 ПК 2.6 У З		ПК 2.5 ПК 2.6 У З
Тема 3.5. Криптозащита информации в сетях передачи данных	Устный опрос. Практические работы № 22	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 3.6. Защита информации в электронных платежных системах	Устный опрос. Практические работы № 23	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З
Тема 3.7. Компьютерная стеганография	Устный опрос. Практическая работа № 24	ОК 01-ОК 10 ПК 2.1 ПК 2.2		ОК 01-ОК 10 ПК 2.1 ПК 2.2	экзамен	ОК 01-ОК 10 ПК 2.1 ПК 2.2

		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З		ПК 2.3 ПК 2.4 ПК 2.5 ПК 2.6 У З

2. Контрольно-оценочные средства (кос) для текущего контроля знаний, умений обучающихся

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

Критерии оценки

«**Отлично**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«**Хорошо**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«**Удовлетворительно**» ставится, если:

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

«**Неудовлетворительно**» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах);
- знания отсутствуют, речь неграмотная

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

(ОК 8, ПК 2.1-2.6).

Тема 1.1 Предмет и задачи программно-аппаратной защиты информации.

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

Тема 1.2 Стандарты безопасности.

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

2. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты).

3. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Тема 1.3 Защищенная автоматизированная система.

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

Тема 1.4 Дестабилизирующее воздействие на объекты защиты.

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

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

1. Понятие несанкционированного доступа к информации. 2. Основные подходы к защите информации от НСД.

3. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.

4. Доступ к данным со стороны процесса.

5. Особенности защиты данных от изменения. Шифрование.

Типовые задания для оценки знаний, умений тесты по разделу 1

(ОК 8, ПК 2.1-2.6).

Тест

Часть А. Вопросы закрытого типа (выбор правильного варианта)

Вопрос №1: Как называется механизм защиты информации, обеспечивающий контроль целостности программного обеспечения?
Варианты ответа:
A. Шифрование
B. Мониторинг активности приложений
C. Контроль целостности файлов
D. Антивирусная защита
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №2: Что означает термин «бэкап» в области информационной безопасности?
Варианты ответа:
A. Процесс шифрования данных
B. Резервное копирование данных
C. Метод анализа уязвимости системы
D. Запись журналов аудита
Компетенции: ПК 2.4, ОК 8

Вопрос №3: Какой тип атаки характеризуется несанкционированным доступом к ресурсам сети путем подделывания IP-адреса отправителя?
Варианты ответа:
A. Атака методом подбора пароля
B. Межсетевое сканирование
C. Подмена адреса (IP-спуфинг)
D. Фишинговая атака
Компетенции: ПК 2.6, ОК 8

Часть Б. вопросы закрытого типа с множественным выбором

Вопрос №4: Какие из перечисленных мер относятся к методам защиты информации от несанкционированного доступа?
Варианты ответа:
A. Использование брандмауэра
B. Применение межсетевых экранов
C. Регулярное резервное копирование данных
D. Биометрический контроль доступа
E. Парольная аутентификация пользователей
F. Логирование сетевого трафика
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №5: Что из перечисленного относится к средствам предотвращения компрометации ключей шифрования?
Варианты ответа:
A. Регулярные обновления антивируса
B. Многократное резервное копирование ключа

C. Физическое ограничение доступа к хранилищу ключей
D. Хэширование передаваемых сообщений
E. Двойная аутентификация (2FA)
F. Периодическая смена секретных ключей
Компетенции: ПК 2.1, ПК 2.3, ОК 8

Вопрос №6: Какие меры используются для минимизации рисков компьютерной атаки («DDoS»)?
Варианты ответа:
A. Расширение пропускной способности каналов связи
B. Распределенные отказоустойчивые архитектуры серверов
C. Активные фильтры сетевого трафика
D. Ограничение числа подключений к одному IP адресу
E. Повышение производительности вычислительных мощностей сервера
F. Инсталляция операционных систем последних версий
Компетенции: ПК 2.6, ОК 8

Часть В. Вопросы открытого типа (краткий ответ)

Вопрос №7: Назовите три метода криптографической защиты информации.

_____

Компетенции: ПК 2.2, ОК 8

Вопрос №8: Перечислите основные виды угроз безопасности информации.

_____

Компетенции: ПК 2.2, ОК 8

Часть Г. Вопросы закрытого типа с сопоставлением

Вопрос №9: Соотнесите типы угроз с соответствующими методами защиты:
Типы угроз:

1. Утечка конфиденциальной информации
2. Нарушение целостности данных
3. Угроза несанкционированного доступа
4. Потеря доступности ресурсов

Методы защиты:
А. Шифрование данных и управление правами доступа
Б. Контроль целостности файлов и аудит изменений
В. Двухфакторная аутентификация и биометрия
Г. Резервное копирование и кластеризация серверов
Компетенции: ПК 2.1, ПК 2.2, ПК 2.4, ОК 8

Вопрос №10: Определите соответствие типов атак и защитных механизмов:
Атаки:

1. Phishing (Фишинг)
2. SQL Injection (SQL-инъекция)
3. Cross-Site Scripting (XSS)
4. Denial of Service (DoS/DDoS)

A. SSL/TLS-шифрование и обучение сотрудников
Б. Валидация ввода данных и экранирование символов
В. Политики Content Security Policy (CSP) и фильтрация вывода

Г. Лимиты соединений и распределённые DNS-серверы

Компетенции: ПК 2.2, ПК 2.6, ОК 8

Ключ

1.	C
2.	B
3.	C
4.	Симметричное шифрование, асимметричное шифрование, хеширование
5.	угрозы утечки конфиденциальной информации, угроза потери доступности ресурсов, угроза нарушения целостности данных
6.	A, B, D, E
7.	C, F
8.	A, B, C, D
9.	1-А, 2-Б, 3-В, 4-Г
10.	1-А, 2-Б, 3-В, 4-Г

Раздел 2. Защита автономных автоматизированных систем

(ОК 8, ПК 2.1-2.6).

Тема 2.1 Основы защиты автономных автоматизированных систем.

1. Работа с автономной АС в защищенном режиме.
2. Алгоритм загрузки ОС. Штатные средства замыкания среды.
3. Расширение BIOS как средство замыкания программной среды.
4. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка).
5. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.

Тема 2.2 Защита программ от изучения.

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

Тема 2.3 Вредоносное программное обеспечение.

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

Тема 2.4 Защита программ и данных от несанкционированного копирования.

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

Тема 2.5 Защита информации на машинных носителях.

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

Тема 2.6 Аппаратные средства идентификации и аутентификации пользователей.

1. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ.

2.Устройства Touch Memory.

Тема 2.7 Системы обнаружения атак и вторжений.

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

Типовые задания для оценки знаний, умений (текущий контроль) тесты по разделу 2 (ОК 8, ПК 2.1-2.6).

Тест

Часть А. Вопросы закрытого типа (выбор правильного варианта)

Вопрос №1: Какие из нижеперечисленных компонентов входят в состав автономного автоматизированного комплекса обработки информации?

Варианты ответа:

A. Сервер хранения данных

B. Рабочая станция пользователя

C. Внешняя система мониторинга

D. Беспроводная точка доступа

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №2: Чем отличается автономная автоматизированная система от сетевой?

Варианты ответа:

A. Автономная система функционирует независимо от внешней среды и централизованных сетей передачи данных.

B. Автономная система обязательно должна иметь физическую связь с внешним миром.

C. Только автономная система имеет встроенную систему контроля доступа.

D. Автономная система требует постоянного подключения к Интернету.

Компетенции: ПК 2.2, ОК 8

Вопрос №3: Какие методы применяются для повышения надежности и устойчивости автономных автоматизированных систем?

Варианты ответа:

A. Ручное создание резервных копий вручную пользователями.

B. Установленные правила периодического автоматического архивирования данных.

C. Организация открытых точек доступа Wi-Fi.

D. Интеграция системы с облачными сервисами.

Компетенции: ПК 2.4, ОК 8

Часть Б. Вопросы открытого типа (краткий ответ)

Вопрос №4: Перечислите три основные цели защиты автономных автоматизированных систем.

_____

Компетенции: ПК 2.1, ОК 8

Вопрос №5: Опишите простой способ защиты рабочих станций автономных автоматизированных систем от вредоносного ПО.

Компетенции: ПК 2.1, ОК 8

Часть В. вопросы закрытого типа с множественным выбором

Вопрос №6: Выберите основные компоненты эффективной системы защиты автономных автоматизированных систем:

Варианты ответа:

A. Средства резервного копирования данных

B. Антивирусные программы и файерволлы

C. Открытые беспроводные сети

D. Управление доступом и авторизацией

E. Отсутствие регулярного обновления ПО

F. Возможность физического доступа посторонних лиц

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №7: Какие из указанных мероприятий способствуют повышению безопасности автономных автоматизированных систем?

Варианты ответа:

A. Ограничение физического доступа к серверам и рабочим станциям

B. Проведение регулярных проверок и тестирования систем защиты

C. Частое изменение настроек безопасности и отключение системных сервисов

D. Регулярный сбор и анализ событий безопасности (логов)

E. Полностью открытое подключение к внешнему Интернету

F. Отказ от резервного копирования данных

Компетенции: ПК 2.2, ПК 2.6, ОК 8

Часть Г. Вопросы закрытого типа с сопоставлением

Вопрос №8: Соотнесите угрозы безопасности автономных автоматизированных систем с рекомендуемыми мерами защиты:

Угрозы:

1. Некорректная работа персонала
2. Несанкционированный физический доступ
3. Заражение вирусами и вредоносным ПО
4. Ошибки конфигурации оборудования и ПО

Средства защиты:

А. Контроль физического доступа (карточки доступа, видеонаблюдение)

Б. Настройка резервного копирования и восстановительные процедуры

В. Информирование сотрудников, обучение правилам безопасности

Г. Регулярное обновление антивирусных баз и системных патчей

Д. Проверка и коррекция конфигураций, контроль над изменениями

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос№9: Установите соответствие между компонентами автономной автоматизированной системы и видами защиты, применяемыми к ним:

Компоненты:

1. Система управления базой данных
2. Пользовательские рабочие станции
3. Интерфейсы взаимодействия оператора с системой
4. Серверы хранения данных

Виды защиты:

А. Мониторинг событий безопасности и журналирование действий операторов

Б. Авторизация и аутентификация пользователей, права доступа

В. Защищённое соединение клиент-сервер (например, TLS/SSL)

Г. Шифрование хранимых данных и регулярное резервное копирование

Компетенции: ПК 2.2, ПК 2.4, ОК 8

Вопрос №10: Соответствие между типами потенциальных угроз и профилактическими мероприятиями:

Угрозы:

1. Вредоносное программное обеспечение
2. Внутреннее нарушение безопасности персоналом
3. Нарушения вследствие технических сбоев оборудования
4. Взлом периферийных устройств

Мероприятия:

А. Регулярное резервное копирование данных и аварийное восстановление

Б. Обучение сотрудников основам информационной безопасности

В. Установка антивирусных решений и антишпионских инструментов

Г. Ограничение физического доступа к оборудованию и соблюдение стандартов эксплуатации

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Ключ

1.	B
2.	A
3.	B
4.	A, B, D
5.	A, B, D
6.	1—B, 2—A, 3—Г, 4—Д
7.	обеспечение конфиденциальности, целостность данных, доступность системы
8.	Регулярное проведение полного сканирования антивирусом, установка обновлений операционной системы и установленных программ, запрет запуска исполняемых файлов неизвестного происхождения.
9.	1—Г, 2—Б, 3—В, 4—А
10.	1—В, 2—Б, 3—А, 4—Г

Раздел 3. Защита информации в локальных сетях (ОК 8, ПК 2.1-2.6).

Тема 3.1 Основы построения защищенных сетей.

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

Тема 3.2 Средства организации VPN.

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

Типовые задания для оценки знаний, умений тесты по разделу 3. (ОК 8, ПК 2.1-2.6).

Тест

Часть А. Вопросы закрытого типа (выбор правильного варианта)

Вопрос №1: Какой протокол используется для безопасной передачи данных по сети?
Варианты ответа:
A. HTTP
B. FTP
C. SMTP
D. SSH
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №2: Для чего предназначен межсетевой экран (брандмауэр)?
Варианты ответа:
A. Блокировка нежелательного веб-контента
B. Изоляция сегментов сети друг от друга
C. Определение местонахождения устройства в сети
D. Автоматическое обновление программного обеспечения
Компетенции: ПК 2.2, ОК 8

Вопрос №3: Что понимается под защитой периметра сети?
Варианты ответа:
A. Обнаружение вирусов внутри рабочей станции
B. Безопасность внешнего соединения сети с Internet
C. Шифрование внутреннего трафика сети
D. Контроль доступа пользователей к отдельным устройствам
Компетенции: ПК 2.6, ОК 8

Часть Б. Вопросы открытого типа (краткий ответ)

Вопрос №4: Какие существуют методы идентификации пользователей в локальной сети?

Компетенции: ПК 2.2, ОК 8

Вопрос №5: Что такое сегментация сети и какая цель её использования?

Компетенции: ПК 2.2, ОК 8

Задание №6: Опишите шаги для настройки брандмауэра в корпоративной сети для повышения безопасности.

Компетенции: ПК 2.1, ПК 2.6, ОК 8

Часть В. вопросы закрытого типа с множественным выбором

Вопрос №7: Какие технологии защищают трафик в локальных сетях от прослушивания?
Варианты ответа:
A. WEP (Wired Equivalent Privacy)
B. WPA/WPA2 (Wi-Fi Protected Access)
C. VLAN (Virtual Local Area Networks)
D. Open Wireless
E. DHCP (Dynamic Host Configuration Protocol)
F. Firewall (Межсетевой экран)
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №8: Какие из приведённых технологий помогают повысить безопасность локальной сети?
Варианты ответа:
A. IPSec (Internet Protocol Security)
B. NAT (Network Address Translation)
C. IDS/IPS (Intrusion Detection System / Intrusion Prevention System)
D. DHCP Server
E. Proxy server
F. File sharing services
Компетенции: ПК 2.2, ПК 2.6, ОК 8

Вопрос №9: Какие элементы инфраструктуры необходимы для полноценной реализации VPN-сети?
Варианты ответа:
A. Маршрутизаторы и коммутаторы
B. Специализированное оборудование для шифрования (VPN Gateway)
C. Веб-сервер для публикации внутренних ресурсов
D. Сервер сертификатов PKI (Public Key Infrastructure)
E. Консольные порты компьютеров
F. Протоколы маршрутизации OSPF/EIGRP/BGP
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Часть Г. Вопросы закрытого типа с сопоставлением

Вопрос №10: Соотнесите категории сетевых атак с основными способами защиты от них:

Категории атак:

1. DoS/DDoS (Denial-of-service attacks)
2. MITM (Man-in-the-Middle Attacks)
3. XSS (Cross-site scripting)
4. SQL Injection

Способы защиты:

А. Патчи и исправления уязвимостей СУБД

Б. SSL/TLS шифрование и строгая политика cookie-файлов

В. Фильтрация входящего трафика и лимитирование запросов

Г. Ввод данных с экранированием спецсимволов и использование параметризованных запросов

Компетенции: ПК 2.2, ПК 2.6, ОК 8

Ключ

1	D
2	B
3	B
4	Пароль, смарт-карты, биометрика (отпечаток пальца, распознавание лица), USB-токены, одноразовые пароли (OTP).
5	Сегментация сети — разделение единой сети на отдельные логические части (подсети). Цель — повышение уровня безопасности, снижение нагрузки на сеть и улучшение управляемости.
6	Необходимо определить политику безопасности, настроить фильтрацию пакетов, ограничить доступ к внутренним ресурсам из Интернета, установить доверенные зоны и маршруты, периодически проверять эффективность правил.
7	A, B, C, F
8	A, B, C, E
9	A, B, D
10	1—В, 2—Б, 3—Б, 4—Г

Раздел 4. Защита информации в сетях общего доступа (ОК 8, ПК 2.1-2.6).

Тема 4.1 Обеспечение безопасности межсетевого взаимодействия.

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

Раздел 5. Защита информации в базах данных

Тема 5.1 Защита информации в базах данных.

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

Тема 5.2 Мониторинг систем защиты.

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

Тема 5.3 Изучение мер защиты информации в информационных системах.

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

Типовые задания для оценки знаний, умений,
тесты по разделу 4 и 5. (ОК 8, ПК 2.1-2.6)

Тест

Часть А. Вопросы закрытого типа (выбор правильного варианта)

Вопрос №1: Какой стандарт применяется для защиты информации в беспроводных сетях общего пользования?

Варианты ответа:

A. WEP

B. WPA3

C. Bluetooth

D. Ethernet

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №2: Что из следующего является примером активной атаки в сетях общего доступа?

Варианты ответа:

A. Sniffing (прослушивание)

B. ARP spoofing (подмена адресов)

C. Анализ трафика

D. Pinging (определение доступности узла)

Компетенции: ПК 2.6, ОК 8

Вопрос №3: Что такое принцип минимальных привилегий применительно к управлению доступом в базах данных?

Варианты ответа:

A. Каждый пользователь получает максимальный доступ ко всей информации

B. Пользователям предоставляются минимальные права, необходимые для выполнения обязанностей

C. Все сотрудники имеют одинаковые полномочия в доступе к данным

D. Информация хранится без какого-либо разграничения прав доступа

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №4: Что подразумевает понятие "целостность данных"?

Варианты ответа:

A. Возможность просмотра данных всеми сотрудниками компании

B. Постоянная доступность данных в любое время суток

C. Корректность и непротиворечивость данных

D. Неограниченный доступ к базам данных без регистрации

Компетенции: ПК 2.2, ОК 8

Часть Б. Вопросы открытого типа (краткий ответ)

Вопрос №5: Опишите процесс настройки VPN для безопасного подключения к корпоративной сети через сеть общего доступа.

_____

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №6: Что такое индексирование в базе данных?

_____

Компетенции: ПК 2.1, ОК 8

Вопрос №7: Какие базовые рекомендации следует соблюдать пользователям при работе в сетях общего доступа?

_____

Компетенции: ПК 2.2, ОК 8

Часть В. вопросы закрытого типа с множественным выбором

Вопрос №8: Какие методы рекомендуется использовать для защиты баз данных от несанкционированного доступа?
Варианты ответа:
A. Строгая политика паролей
B. Однократная аутентификация
C. Реализация механизма шифрования
D. Предоставление максимальных прав доступа сотрудникам
E. Ограничение количества активных сессий
F. Запрет на журналы аудита
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №9: Какие типы атак наиболее распространены против баз данных?
Варианты ответа:
A. Перебор паролей (Brute Force attack)
B. SQL-инъекции
C. Overflow атаки (атаки переполнения буфера)
D. Электронная почта спама
E. Физическое повреждение жёстких дисков
F. Social engineering (социальная инженерия)
Компетенции: ПК 2.2, ПК 2.6, ОК 8

Вопрос №10: Какие факторы влияют на степень защищённости базы данных?
Варианты ответа:
A. Уровень квалификации разработчиков и администраторов
B. Сложность алгоритмов шифрования
C. Географическое расположение сервера
D. Количество одновременных обращений к базе данных
E. Степень автоматизации процессов резервного копирования
F. Наличие выделенного специалиста по кибербезопасности
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №11: Какие уровни авторизации существуют в большинстве современных баз данных?
Варианты ответа:
A. Администратор
B. Читатель
C. Редактор
D. Гость

E. Менеджер базы данных
F. Разработчик интерфейсов
Компетенции: ПК 2.2, ОК 8

Часть Г. Вопросы закрытого типа с сопоставлением

Вопрос №12: Соотнесите виды атак на базы данных с их описанием:
Вид атаки:

1. SQL-инъекция
2. Атака перебором (Brute force)
3. Атака отказа в обслуживании (DoS/DDoS)
4. Атака переполнения буфера (Buffer overflow)

Описание:
А. Преобразование обычного запроса к базе данных в злонамеренный с целью получения или изменения данных
Б. Массированные запросы, направленные на перегрузку ресурса и прекращение обслуживания легитимных клиентов
В. Повторное выполнение множества неудачных попыток входа с целью подобрать пароль
Г. Передача большого объёма данных, превышающего размер памяти переменной, приводящее к выполнению произвольного кода
Компетенции: ПК 2.2, ПК 2.6, ОК 8

Вопрос №13: Установите соответствие между элементами базы данных и целями защиты:
Элементы базы данных:

1. Таблицы и записи
2. Связи между объектами данных
3. Конфигурационные файлы и схемы
4. Доступ к журналам операций и транзакций

Цели защиты:
А. Сохранение структуры данных и связей между ними
Б. Надежность резервного копирования и возможность восстановления данных
В. Целостность и сохранность самих данных
Г. Ограничение неправомерного доступа к информации о действиях пользователей и изменениях в базе данных
Компетенции: ПК 2.1, ПК 2.2, ОК 8

Вопрос №14: Связать роли пользователей с их полномочиями в базе данных:
Роли пользователей:

1. Администратор
2. Пользователь-чтец
3. Редактор
4. Гость

Полномочия:
А. Может просматривать данные, но не изменять их
Б. Имеет полный доступ к изменению, созданию и удалению объектов базы данных
В. Нет доступа к просмотру или редактированию данных
Г. Может вносить изменения в существующие объекты базы данных
Компетенции: ПК 2.2, ОК 8

Вопрос №15: Подберите соответствующие защитные механизмы для каждого вида угрозы:
Угрозы:

1. Случайное удаление важной информации
2. Утечка данных из-за слабых паролей
3. Неправильная конфигурация доступа
4. Инфраструктура атаки на серверы базы данных

Механизмы защиты:

А. Режимы ограничения прав доступа и чёткая политика предоставления привилегий

Б. Регулярные архивные копии и контроль версий

В. Обязательная двухфакторная аутентификация и надёжные пароли

Г. Применять своевременные обновления ОС и регулярно проводить аудит системы безопасности

Компетенции: ПК 2.1, ПК 2.2, ОК 8

Ключ

1.	B
2.	B
3.	B
4.	C
5.	Установка специализированного клиента VPN, получение сертификата безопасности, настройка параметров подключения (сервер, порт, используемый протокол), включение автоматической активации VPN при входе в сеть общего доступа, постоянное поддержание актуальной версии программного обеспечения VPN.
6.	Индексирование — это структура данных, ускоряющая операции выборки записей из таблицы.
7.	Использование VPN-сервисов, активация шифрования данных, избегание передачи чувствительной информации, проверка сертификатов безопасности
8.	A, C, E
9.	A, B, C, F
10.	A, B, E, F
11.	A, B, C, D, E
12.	1—A, 2—B, 3—Б, 4—Г
13.	1—B, 2—A, 3—Б, 4—Г
14.	1—Б, 2—A, 3—Г, 4—B
15.	1—Б, 2—B, 3—A, 4—Г

Экзаменационные вопросы

1. Предмет и задачи программно-аппаратной защиты информации.
2. Классификация методов и средств программно-аппаратной защиты информации.
3. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
4. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.
5. Методы создания безопасных систем.
6. Методология проектирования гарантированно защищенных КС.
7. Источники дестабилизирующего воздействия на объекты защиты.
8. Причины и условия дестабилизирующего воздействия на информацию.
9. Понятие несанкционированного доступа к информации. Основные подходы к защите информации от НСД.
10. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
11. Особенности защиты данных от изменения. Шифрование.
12. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка).
13. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.
14. Задачи защиты ПО от изучения и способы их решения. Защита ПО от дизассемблирования.
15. Вредоносное программное обеспечение как особый вид разрушающих воздействий. Классификация вредоносного программного обеспечения.
16. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения.
17. Поиск следов активности вредоносного ПО.
18. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. 19. Ботнеты. Принцип функционирования. Методы обнаружения.
20. Классификация антивирусных средств. Сигнатурный и эвристический анализ. 21. Защита от вирусов в "ручном режиме".
22. Основные концепции построения систем антивирусной защиты на предприятии.
23. Несанкционированное копирование программ как тип НСД.
24. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.
25. Защитные механизмы в современном программном обеспечении на примере MS Office.
26. Проблема защиты отчуждаемых компонентов ПЭВМ.
27. Методы защиты информации на отчуждаемых носителях. Шифрование.
28. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.
29. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.
30. Безвозвратное удаление данных. Принципы и алгоритмы.
31. Устройства Touch Memory.
32. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.
33. Использование сетевых снифферов в качестве СОВ.
34. Аппаратный компонент СОВ. Программный компонент СОВ.
35. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий.
36. Штатные средства защиты информации стека протоколов TCP/IP.

37. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

38. Виртуальная частная сеть. Функции, назначение, принцип построения. 39. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.

40. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.

41. Основные типы firewall. Симметричные и несимметричные firewall.

42. Однохостовые и мультихостовые firewall.

43. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту, исходя из архитектуры и выполняемых функций.

44. Основные типы угроз. Модель нарушителя.

45. Средства идентификации и аутентификации. Управление доступом. 46. Средства контроля целостности информации в базах данных.

47. Средства аудита и контроля безопасности. Критерии защищенности баз данных.

48. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.

49. Классификация сетевых мониторов.

50. Системы управления событиями информационной безопасности (SIEM).

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

Устный опрос.

Практические занятия. Оценка освоения дисциплины предусматривает проведение экзамена.

I. ПАСПОРТ

Назначение:

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

- 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;

− устанавливать, настраивать, применять программные и программно- ппаратные средства защиты 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

Знания

− 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;

− 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 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.

ОК 8 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

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

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

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

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

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

ПК 2.6 - Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

II. ВОПРОСЫ ДЛЯ ЭКЗАМЕНА

1. Основные понятия программно-аппаратной защиты информации
2. Классификация методов и средств программно-аппаратной защиты информации
3. Стандарты по защите информации
4. Автоматизация процесса обработки информации
5. Основные виды АС в защищенном исполнении
6. Методы создания безопасных систем
7. Учет, обработка, хранение и передача информации в АИС
8. Моделирование угроз и рисков для защищенной автоматизированной системы
9. Идентификация и аутентификация пользователей
10. Криптографическая защита
11. Способы воздействия на информацию
12. Исследование несанкционированного доступа к информации
13. Защита информации от несанкционированного доступа
14. Шифрование данных различными методами
15. Разработать простой алгоритм шифрования и дешифрования информации
16. Способы изучения ПО
17. Вредоносное программное обеспечение как особый вид разрушающих воздействий
18. Классификация вредоносного ПО
19. Схема заражения компьютеров вредоносным ПО
20. Основные концепции построения систем антивирусной защиты на предприятии
21. Методы защиты информации на отчуждаемых носителях
22. Безвозвратное удаление данных
23. Средства восстановления информации
24. Несанкционированный доступ к носителю
25. Применение специализированного программного средства для восстановления удаленных файлов
26. СОВ и СОА, отличия в функциях
27. Методы обнаружения вторжений

28. Моделирование проведения атаки
29. Виртуальная частная сеть
30. Устройства, образующие VPN
31. Средства организации VPN
32. Межсетевые экраны типа firewall
33. Обеспечение безопасности межсетевого взаимодействия
34. Различные способы закрытия "опасных" портов
35. Основные типы угроз. Модель нарушителя
36. Исследование основных типов угроз, модель нарушителя
37. Понятие и обоснование необходимости использования мониторинга
38. Классификация сетевых мониторов
39. Проведение аудита ЛВС сетевым сканером
40. Создание архитектуры компьютера
41. Системный блок и его компоненты
42. Анализ пользовательского интерфейса
43. Разработка концепции нового устройства

Критерии оценок:

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

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

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

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

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

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

Устный опрос.

Практические занятия.

Оценка освоения дисциплины предусматривает проведение экзамена.

I. ПАСПОРТ

Назначение:

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

Умения

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

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

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

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

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

У6 - применять математический аппарат для выполнения криптографических преобразований;

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

У8 - применять средства гарантированного уничтожения информации;

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

У10 - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Знания

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

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

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

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

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

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

ОК 1 - Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

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

ОК 3 - Планировать и реализовывать собственное профессиональное и личностное развитие.

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

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

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

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

ОК 8 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9 - Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

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

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

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

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

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

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

ПК 2.6 - Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

II. ВОПРОСЫ ДЛЯ ЭКЗАМЕНА

1. Предмет и задачи криптографии. История криптографии. Основные термины.
2. Элементы теории множеств. Группы, кольца, поля.
3. Делимость чисел. Признаки делимости. Простые и составные числа.
4. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа.

Алгоритм Евклида для нахождения НОД.

5. Отношения сравнимости. Свойства сравнений. Модулярная арифметика. 6. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма -Эйлера. Алгоритм быстрого возведения в степень по модулю.
7. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений
8. Способы кодирования информации и шифрование
9. Решение линейных диофантовых уравнений
10. Проверка чисел на простоту
11. Решение задач с элементами теории чисел
12. Арифметические операции над большими числами
13. Классификация основных методов криптографической защиты. Методы симметричного шифрования.
14. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.
15. Методы перестановки. Табличная перестановка, маршрутная перестановка.
16. Применение классических шифров замены
17. Применение классических шифров перестановки

18. Применение метода гаммирования
19. Основные методы криптоанализа. Криптографические атаки.
20. Криптоанализ шифра простой замены методом анализа частотности символов
21. Криптоанализ классических шифров методом полного перебора ключей
22. Криптоанализ шифра Виженера
23. Основные принципы поточного шифрования
24. Применение методов генерации ПСЧ
25. Способы получения псевдослучайных последовательностей
26. Кодирование информации. Символьное кодирование. Смысловое кодирование.
27. Компьютеризация шифрования. Аппаратное и программное шифрование.
28. Изучение современных программных и аппаратных криптографических средств.
29. Кодирование информации
30. Программная реализация классических шифров
31. Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге
32. Общие сведения. Структурная схема симметричных криптографических систем.
33. Изучение программной реализации современных симметричных шифров
34. Однонаправленные хеш-функции. Алгоритмы цифровой подписи. Применение различных функций хеширования, анализ особенностей хешей
35. Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.
36. Применение протокола Диффи-Хеллмана для обмена ключами шифрования
37. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр.
38. Применение генерации ключей
39. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.
40. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей
41. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.
42. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ

Критерии оценок:

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

– оценка **«хорошо»**, если студент обладает достаточно полным знанием программного материала; его ответ представляет грамотное изложение учебного

материала; но имеются существенные неточности в формулировании понятий и закономерностей по вопросам; не полностью сделаны выводы по излагаемому материалу;

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

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

Критерии оценок:

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

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

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

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

Вопросы для устного опроса по темам

Критерии оценки

«**Отлично**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять

существенные и несущественные моменты материала.

«**Хорошо**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«**Удовлетворительно**» ставится, если:

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

«**Неудовлетворительно**» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах);
- знания отсутствуют, речь неграмотная

Тема 1.1 Введение. Математические основы криптографии

1. Предмет и задачи криптографии. История криптографии. Основные термины.
2. Элементы теории множеств. Группы, кольца, поля.
3. Делимость чисел. Признаки делимости. Простые и составные числа.
4. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа.

Алгоритм Евклида для нахождения НОД.

5. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.
6. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма - Эйлера. Алгоритм быстрого возведения в степень по модулю.

Тема 2.1 Методы криптографической защиты информации.

1. Классификация основных методов криптографической защиты. Методы симметричного шифрования.
2. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.
3. Методы перестановки. Табличная перестановка, маршрутная перестановка.

Тема 2.2. Криптоанализ

1. Основные методы криптоанализа. Криптографические атаки.

Тема 2.3 Поточные шифры и генераторы псевдослучайных чисел

1. Основные принципы поточного шифрования

Тема 3.1 Кодирование информации. Компьютеризация шифрования

1. Кодирование информации. Символьное кодирование. Смысловое кодирование.
2. Компьютеризация шифрования. Аппаратное и программное шифрование.

Тема 3.2 Симметричные системы шифрования

1. Общие сведения. Структурная схема симметричных криптографических систем.

Тема 3.3 Асимметричные системы шифрования

1. Однонаправленные хеш-функции. Алгоритмы цифровой подписи

Тема 3.5 Алгоритмы обмена ключей и протоколы аутентификации

1. Задание для устного опроса по темам 1. Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.

Тема 3.6 Криптозащита информации в сетях передачи данных

1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр.

Тема 3.7 Защита информации в электронных платежных системах

1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.

Тема 3.8. Компьютерная стеганография.

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

Экзаменационные вопросы

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

современных программных и аппаратных криптографических средств.

27. Общие сведения. Структурная схема симметричных криптографических систем 28. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

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

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

31. Элементы теории чисел в криптографии с открытым ключом.

32. Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи

33. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.

34. Взаимная аутентификация. Односторонняя аутентификация

35. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.

36. Криптомаршрутизатор. Пакетный фильтр

37. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.

38. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер

39. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.

40. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.

41. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ

Типовые задания для оценки знаний, умений

(ОК 8, ПК 2.1-2.6).

Тест

Часть А. Закрытый тип (выбор правильного ответа):

Вопрос 1: Что такое симметричное шифрование?

A) Используется одна и та же секретная ключевая последовательность для зашифровки и расшифровки данных.

B) Используется два ключа: открытый и закрытый.

C) Это способ сжатия данных перед передачей.

D) Метод распределения ключей.

Компетенции: ПК 2.2, ОК 2

*Вопрос 2:*Какие преимущества имеет асимметричная система шифрования?

A) Высокая скорость шифрования и дешифрации.

B) Простота распространения открытых ключей.

C) Возможность быстрого восстановления потерянных ключей.

D) Легкость установки.

Компетенции: ПК 2.2, ОК 2

*Вопрос 3:*Что представляет собой хэш-функция?

A) Алгоритм шифрования, используемый для преобразования текста в зашифрованный вид.

B) Процедура для сокрытия исходного содержимого файла.

C) Функция, преобразующая произвольный объём данных в фиксированный уникальный код.

D) Средство контроля за работой компьютеров.

Компетенции: ПК 2.2, ОК 2

*Вопрос 4:*В чём заключается основное отличие электронной цифровой подписи (ЭЦП) от простой цифровой подписи?
A) ЭЦП позволяет однозначно определить автора документа и подтвердить целостность информации.
B) Электронная подпись обязательна только для юридических лиц.
C) Обычные подписи удобнее для повседневного использования.
D) ЭЦП менее надежна и чаще подделывается.
Компетенции: ПК 2.2, ОК 2

*Вопрос 5:*Какие существуют способы хранения закрытых ключей в асимметричной криптосистеме?
A) Хранение на бумажном носителе.
B) Использование смарт-карты или токена.
C) Запись на внешний жесткий диск.
D) Все вышеперечисленные варианты верны.
Компетенции: ПК 2.1, ОК 2

*Вопрос 6:*Какой алгоритм шифрования применяется в ГОСТ Р 34.12-2015?
A) AES
B) RSA
C) KUZNYECHIK
D) SHA-256
Компетенции: ПК 2.2, ОК 2

*Вопрос 7:*В каком случае целесообразно использование гибридной криптографической схемы?
A) Когда нужно повысить производительность алгоритма симметричного шифрования.
B) Когда необходимо обеспечить высокую степень защиты больших объемов данных.
C) Только при передаче небольших объемов данных.
D) Всегда предпочтительнее любого другого метода.
Компетенции: ПК 2.2, ОК 2

*Вопрос 8:*Какие меры необходимы для надежной защиты закрытой части сертификата открытого ключа?
A) Её следует хранить в открытом доступе для удобства проверки подлинности.
B) Закрытая часть должна храниться отдельно от открытой части и защищаться физически и программно.
C) Она вообще не подлежит защите, поскольку доступна любому желающему.
D) Достаточно обычного антивирусного сканера.
Компетенции: ПК 2.1, ОК 2

*Вопрос 9:*Как осуществляется проверка подлинности электронного документа с помощью цифровой подписи?
A) Путём сравнения подписанного документа с открытым текстом оригинала.

B) Подпись проверяется путём вычисления хэша документа и сверки его с оригинальной подписью.
C) Подписанный документ автоматически отправляется владельцу оригинального документа.
D) Цифровая подпись хранится на специальном сервере, откуда запрашиваются данные для проверки.
Компетенции: ПК 2.2, ОК 2

*Вопрос 10:*Какова основная цель протокола SSL/TLS?
A) Предназначен для сжатия данных перед передачей по каналам связи.
B) Служит для предоставления публичного пространства пользователям Интернета.
C) Обеспечивает конфиденциальность и целостность данных при обмене информацией по сети Интернет.
D) Протокол предназначен исключительно для корпоративных сетей.
Компетенции: ПК 2.2, ОК 2

Часть Б.Открытый тип (краткий ответ):

Вопрос 11: Перечислите три наиболее распространённые угрозы безопасности данных в современных условиях.

_____
Компетенции: ПК 2.2, ОК 2

Вопрос 12: Приведите пример алгоритма симметричного шифрования.

_____
Компетенции: ПК 2.2, ОК 2

Вопрос 13: Объясните, зачем нужны контрольные суммы в процессах передачи данных.

_____
Компетенции: ПК 2.2, ОК 2

Вопрос 14: Опишите процесс формирования и проверки цифровой подписи простыми словами.

_____
Компетенции: ПК 2.2, ОК 2

Вопрос 15: Дайте определение стойкости криптографического алгоритма.

_____
Компетенции: ПК 2.2, ОК 2

Вопрос 16: Зачем применяют протокол SSH?

_____
Компетенции: ПК 2.2, ОК 2

Вопрос 17: В чём принципиальное отличие TLS от HTTPS?

Компетенции: ПК 2.2, ОК 2

Вопрос 18: В чём разница между шифром и режимом шифрования?

Компетенции: ПК 2.2, ОК 2

Вопрос 19: Перечислите две основные характеристики надёжного пароля.

Компетенции: ПК 2.2, ОК 2

Вопрос 20: Перечислите ключевые этапы жизненного цикла управления ключами.

Компетенции: ПК 2.1, ОК 2

Часть В. Вопросы закрытого типа с множественным выбором

Вопрос 21: Выберите методы криптографической защиты информации:
A) Шифрование.
B) Хэширование.
C) Логирование ошибок.
D) Дублирование данных.
E) Аутентификация.
Компетенции: ПК 2.2, ОК 2

Вопрос 22: Какие виды атак угрожают симметричному шифрованию?
A) Атака методом перебора.
B) Атака по открытому тексту.
C) Эксплуатация слабостей в управлении ключами.
D) Социальная инженерия.
E) Отказ в обслуживании (DoS/DDoS).
Компетенции: ПК 2.2, ОК 2

Вопрос 23: Какие механизмы защищают инфраструктуру открытых ключей (PKI)?
A) Периодическая смена корневых сертификатов.
B) Физическая охрана центров сертификации.
C) Двухфакторная аутентификация при выдаче сертификатов.
D) Ограничение максимального срока действия сертификатов.
E) Скрытие всей технической документации.
Компетенции: ПК 2.1, ОК 2

Вопрос 24: Какие проблемы возникают при недостаточной длине ключа в криптографическом алгоритме?
A) Увеличенная нагрузка на вычислительные мощности.
B) Рост вероятности успешного вскрытия путем перебора.
C) Трудности с совместимостью старых версий программы.

D) Низкая стойкость к современным методам взлома.
E) Нарушение конфиденциальности данных.
Компетенции: ПК 2.2, ОК 2

Вопрос 25: Отметьте причины, по которым могут потребоваться частые смены криптографических ключей:
A) Ключи становятся известны третьим лицам.
B) Время действия ключа истекло.
C) Произошли изменения в требованиях безопасности.
D) Необходимо сэкономить ресурсы сервера.
E) Пользователь забыл старый пароль.
Компетенции: ПК 2.1, ОК 2

Часть Г. Вопросы закрытого типа с сопоставлением

Вопрос 26: Соотнесите типы криптографических алгоритмов с их примерами
Компетенции: ПК 2.2, ОК 2

Тип	Пример
A. Симметричный алгоритм	1. RSA
B. Асимметричный алгоритм	2. AES
C. Хэш-функция	3. MD5

Вопрос 27: Соотнесите элементы криптографической инфраструктуры с их функциями
Компетенции: ПК 2.1, ОК 2

Элемент	Функция
A. Удостоверяющий центр (CA)	1. Выполняет выдачу и аннулирование сертификатов
B. Репозиторий сертификатов	2. Предоставляет хранилище доверенных сертификатов
C. Ревокашн-сервис (OCSP/CRL)	3. Проверяет статус отзыва сертификатов

Вопрос 28: Соотнесите название криптографического алгоритма с соответствующей страной-разработчиком:
Компетенции: ПК 2.2, ОК 2

Алгоритм	Страна-разработчик
A. AES	1. Бельгия
B. RSA	2. США
C. ГОСТ Р 34.12-2015	3. Россия

Вопрос 29: Соотнесите термин с определением
Компетенции: ПК 2.2, ОК 2

Термин	Определение
A. Эндопараметр	1. Внутреннее значение, которое влияет на устойчивость криптосистемы
B. Стеганография	2. Искусство скрытой передачи информации внутри обычных объектов
C. Манипуляция битами	3. Процесс целенаправленного изменения отдельных битов для обхода криптосистем

Вопрос 30: Соотнесите характеристику с типом криптографического алгоритма
Компетенции: ПК 2.2, ОК 2

Характеристика	Тип алгоритма
A. Один ключ используется для обоих операций (шаг за шагом)	1. Симметричный
B. Два разных ключа применяются для шифрования и расшифровки	2. Асимметричный
C. Нет обратимости результата	3. Хэш-функция

Ключи

1	A
2	B
3	C
4	A
5	D
6	C
7	B
8	B
9	B
10	C
11	Атаки методом подбора пароля, фишинг, вирусы-шифровальщики
12	DES, AES, RC4.
13	Контрольные суммы позволяют проверить целостность данных после передачи и выявить возможные искажения или повреждения.
14	Отправитель формирует цифровую подпись, используя свой закрытый ключ, а получатель проверяет её валидность с помощью открытого ключа отправителя.
15	Стойкость криптографического алгоритма — это способность противостоять попыткам взлома и восстановить оригинальные данные без знания секретного ключа.
16	Протокол SSH служит для безопасной передачи команд и данных по небезопасным сетям, обеспечивая аутентификацию и шифрование
17	TLS — это протокол безопасности, использующийся для защиты соединения, тогда как HTTPS — это расширение HTTP-протокола, работающее поверх TLS для обеспечения безопасности веб-трафика.
18	Шифр — это сам алгоритм шифрования, определяющий правила преобразования данных. Режим шифрования — это способ применения шифра, влияющий на порядок обработки блоков данных.
19	Длина и сложность, включающая разные типы символов (буквы, цифры, знаки препинания).
20	Генерация, распространение, хранение, использование, замена, уничтожение.

21	A, B, E
22	A, B, C
23	A, B, C, D
24	B, D, E
25	A, B, C
26	A → 2, B → 1, C → 3
27	A → 1, B → 2, C → 3
28	A → 1, B → 2, C → 3
29	A → 1, B → 2, C → 3
30	A → 1, B → 2, C → 3

4. Требования к дифференцированному зачету по учебной и (или) производственной практике

Дифференцированный зачет по учебной и (или) производственной практике выставляется с учетом данных аттестационного листа (характеристики профессиональной деятельности обучающегося/студента на практике) с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

4.1. Оценочные материалы

Перечень вопросов к собеседованию по производственной практике

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

5. Комплект экзаменационных материалов

Задания для экзаменующегося

Задание 1

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

1. 5., ПК 2.6.

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

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

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

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

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

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно- аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Инструкция

Внимательно прочитайте задание. Время выполнения задания – 40 минут Текст задания:

Вариант № 1

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

Вариант № 2

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

Вариант № 3

Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Вариант № 4

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

Вариант № 5

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

Вариант № 6

Опишите параметры и значения параметров Политики аудита. Просмотрите события в журнале событий. Информация о каких событиях сохраняется в системном журнале? Какие

данные по каждому событию отображаются в журнале? Включите аудит успеха и отказа всех параметров.

Вариант № 7

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

Вариант № 8

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

Вариант № 9

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

Вариант № 10

Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту: ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

ЗАДАНИЕ 2

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

ОК 09, ОК 10

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

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

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

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном

языке.

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания – 40 минут

Вариант 1.

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

Вариант 2.

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

Вариант 3.

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

Вариант 4.

Представьте алгоритм работы российского стандарта шифрования ГОСТ 2 8 1 4 7 - 8 9 . Выполнить ручное шифрование исходного текста с помощью алгоритма ГОСТ 28147-89. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES. Приведите примеры программ симметричного шифрования.

Вариант 5.

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

Вариант 6.

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

Вариант 7.

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

Вариант 8.

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

Вариант 9.

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

Вариант 10.

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

ЗАДАНИЕ 3

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

ОК 09, ОК 10

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

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

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

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания – 40 минут

Вариант 1.

Напишите краткое руководство по основным командам Linux для начинающих пользователей.

Включите примеры использования каждой команды.

Вариант 2.

Исследуйте и сравните три популярных дистрибутива Linux (например, Ubuntu, Fedora и CentOS). Опишите их основные особенности и целевую аудиторию.

Вариант 3.

Установите GRUB на виртуальную машину с Linux. Опишите процесс установки и настройки, а также как добавить новые записи в меню загрузки.

Вариант 4.

Опишите, что такое демоны в Linux. Приведите примеры распространенных демонов и их функций в системе.

Вариант 5.

Напишите сценарий на Bash, который будет отслеживать и выводить информацию о текущих процессах в системе (например, используя команды ps, top и htop).

Вариант 6.

Объясните, как работает файловая система в Linux. Опишите, как создать и отформатировать новый раздел с помощью командной строки.

Вариант 7.

Установите VirtualBox на свою машину и создайте виртуальную машину с Ubuntu. Опишите

процесс установки и настройки параметров виртуальной машины.

Вариант 8.

Установите Debian 11 Desktop на виртуальную машину. Опишите процесс установки, включая выбор пакетов и конфигурацию сети.

Вариант 9.

Напишите краткое руководство по использованию текстовых редакторов Vim и Nano. Включите основные команды для редактирования, сохранения и выхода из редакторов.

Вариант 10.

Используя инструменты командной строки, такие как top, htop и ps, создайте отчет о текущих процессах на вашей системе. Опишите, как интерпретировать полученные данные.

5.1. Пакет экзаменатора

Условия выполнения задания:

Инструкция

Ознакомьтесь с заданиями для экзаменующихся

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

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

Задание № 1–40 минут

Задание № 2–40 минут

Задание № 3–40 минут

Всего на экзамен – 2 часа

Экзамен проводится в группе в количестве - 19 человек

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

5.2. Критерии оценки

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

Параметры оценивания:

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

1.3 Контрольно-оценочные средства для проведения экзамена по модулю

1.3.1 Общие положения

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

Экзамен включает: практический экзамен, защита портфолио.

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

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемых показателям, а также общих компетенций. Условием допуска к экзамену (квалификационному) является положительная аттестация по текущему контролю (защита контрольных работ, тестирование, защита ЛПЗ, решение ситуационных задач) и по промежуточному (МДК.02.01, МДК.02.02, МДК 02.03, учебной практике УП.02 и производственной практике (по профилю специальности ПП.02)).

1.3.2 Таблица сочетаний, проверяемых ПК и ОК:

В результате контроля и оценки по профессиональному модулю осуществляется комплексная проверка следующих профессиональных и общих компетенций:	**Показатели оценки результата**	**Форма экзамена**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации	Выполнены установка и настройка отдельных программных, программно-аппаратных средств защиты информации.	Практическое выполнение задания №1
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Обеспечена защита информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Практическое выполнение задания №1

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Выполнено тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Практическое выполнение задания №1
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	Выполнены обработка, хранение и передача информации ограниченного доступа.	Практическое выполнение задания №1
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Уничтожены информация и носители информации с использованием программных и программно-аппаратных средств.	Практическое выполнение задания №1
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в	Выполнена регистрация основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных	Практическое выполнение задания №1
том числе с использованием программных и программно- аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Обоснован выбор метода и средства решения профессиональной задачи. Дана адекватная оценка и самооценка эффективности и качества выполнения профессиональной задачи.	Практическое выполнение задания №2
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной	Использованы различные источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональной задачи.	Практическое выполнение задания №2

деятельности		
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие	Продемонстрирована ответственность за принятые решения. Обоснованы самоанализ и коррекция результатов собственной работы.	Практическое выполнение задания №2
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентам	Продемонстрирована способность работы в коллективе и команде, взаимодействия с коллегами, руководством, клиентами.	Практическое выполнение задания №2
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Продемонстрирована способность осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Практическое выполнение задания №2
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей	Презентовать структуру профессиональной деятельности по профессии (специальности)	Практическое выполнение задания №2
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Соблюдать нормы экологической безопасности. Определять направления ресурсосбережения в рамках профессиональной деятельности по профессии (специальности)	Практическое выполнение задания №2
ОК 08. Использовать средства физической культуры для	Использовать физкультурно-оздоровительную деятельность для	Практическое выполнение

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

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

Общие компетенции, для проверки сформированности которых используется портфолио: ОК 1, ОК 2, ОК 3, ОК 04, ОК 5, ОК 6, ОК 07, ОК 08, ОК 09, ОК 10.

Требования к портфолио:

Тип портфолио: портфолио смешанного типа, Основные

требования:

Обязательные документы:

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

Дополнительные материалы:

- Доклады участников научно-практических конференций;
- результаты участия во внеурочной научно-исследовательской деятельности;
- Грамоты за спортивные и общественные достижения;
- портфолио в электронном виде (сообщения, рефераты, доклады, отчеты по практическим занятиям, видеоматериалы, фотоматериалы, презентации профессиональной направленности, выполненные обучающимися во время самостоятельной работы);
- свидетельства, подтверждающие участие в коллективных творческих мероприятиях
- (ведущий тематического вечера, член жюри, участник слета, участник турпохода, и т. д.).

Требования к структуре оформлению и защите портфолио:

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

3.6.4 Выполнения задания в ходе экзамена

Комплект экзаменационных материалов

2. Задание для экзаменующегося

Задание 1

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

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

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

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

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

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

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно- аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Инструкция

Внимательно прочитайте задание. Время выполнения задания – 40 минут Текст задания:

Вариант № 1

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

Вариант № 2

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

Вариант № 3

Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Вариант № 4

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

Вариант № 5

Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Установите для этой папки разрешения полного доступа для одного из

пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера. Предложите стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Вариант № 6

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

Вариант № 7

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

Вариант № 8

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

Вариант № 9

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

Вариант № 10

Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту: ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, –

скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

ЗАДАНИЕ 2

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

ОК 09, ОК 10

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

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

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

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном

языке.

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания –

40 минут

Вариант 1.

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

Вариант 2.

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

Вариант 3.

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

Вариант 4.

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

Вариант 5.

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

Вариант 6.

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

Вариант 7.

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

Вариант 8.

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

Вариант 9.

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

Вариант 10.

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

ЗАДАНИЕ 3

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

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

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

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

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания –
40 минут

Вариант 1.

Напишите краткое руководство по основным командам Linux для начинающих пользователей.

Включите примеры использования каждой команды.

Вариант 2.

Исследуйте и сравните три популярных дистрибутива Linux (например, Ubuntu, Fedora и CentOS). Опишите их основные особенности и целевую аудиторию.

Вариант 3.

Установите GRUB на виртуальную машину с Linux. Опишите процесс установки и настройки, а также как добавить новые записи в меню загрузки.

Вариант 4.

Опишите, что такое демоны в Linux. Приведите примеры распространенных демонов и их функций в системе.

Вариант 5.

Напишите сценарий на Bash, который будет отслеживать и выводить информацию о текущих процессах в системе (например, используя команды ps, top и htop).

Вариант 6.

Объясните, как работает файловая система в Linux. Опишите, как создать и отформатировать новый раздел с помощью командной строки.

Вариант 7.

Установите VirtualBox на свою машину и создайте виртуальную машину с Ubuntu. Опишите
процесс установки и настройки параметров виртуальной машины.

Вариант 8.

Установите Debian 11 Desktop на виртуальную машину. Опишите процесс установки, включая выбор пакетов и конфигурацию сети.

Вариант 9.

Напишите краткое руководство по использованию текстовых редакторов Vim и Nano. Включите основные команды для редактирования, сохранения и выхода из редакторов.

Вариант 10.

Используя инструменты командной строки, такие как top, htop и ps, создайте отчет о текущих процессах на вашей системе. Опишите, как интерпретировать полученные данные.

3.6.5 Пакет экзаменатора

Условия выполнения задания:

Инструкция

Ознакомьтесь с заданиями для экзаменующихся

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

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

Задание № 1–40 минут

Задание № 2–40 минут

Задание № 3–40 минут

Всего на экзамен – 2 часа

Экзамен проводится в группе в количестве - 19 человек

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

3.6.6 Критерии оценки

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

Параметры оценивания:

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

Министерство образования и науки Республики Дагестан
Государственное бюджетное профессиональное образовательное учреждение
Республики Дагестан
«Кизлярский профессионально-педагогический колледж»

СОГЛАСОВАНА С РАБОТОДАТЕЛЯМИ:
ООО «Оптимасеть»
наименование предприятия
директор
должность
Магомедов С.А.
(фамилия)

УТВЕРЖДАЮ
зам. директора по учебной работе
Е.Н.Шелкова
«29» 08 2022 г.

Комплект контрольно-оценочных средств

по профессиональному модулю

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

образовательной программы (ОП)

по специальности/

10.02.05 Обеспечение информационной безопасности автоматизированных систем
код, наименование

Рассмотрен и одобрен предметной (цикловой) комиссией профессиональных дисциплин технических специальностей
наименование по приказу

Председатель предметной (цикловой) комиссии
_____ / Раджабова А.Н.
подпись *расшифровка подписи*
29 08 2022 г.

Кизляр, 2022 г.

Комплект контрольно-оценочных средств разработан на основе: Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем входящей в состав УГПС 10.00.00 Информационная безопасность рабочей программы ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Разработчик(и):

Искандырова Ажар Асадулаева
ФИО, должность, место работы

Раджабова Альбина Нязовна
ФИО, должность, место работы

Рекомендована методическим советом ГБПОУ РД «Кизлярский профессионально-педагогический колледж» для применения в учебном процессе.

Заключение методического совета № 1 от 29 08 2022 г.

ОБЩИЕ ПОЛОЖЕНИЯ

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности Защита информации в автоматизированных

системах программными и программно-аппаратными средствами и составляющих его профессиональных компетенций, а также общие компетенции, формирующиеся в процессе освоения основной образовательной программы в целом.

Формой аттестации по профессиональному модулю является экзамен по модулю.

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

Экзамен по модулю проводится в форме выполнения практико-ориентированных заданий.

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
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:

Владеть навыками	− установки, настройки программных средств защиты информации в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностика, устранения отказов и восстановления 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.
Уметь	− 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; − 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 средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

Знать	− 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; − 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 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.

1. ФОРМЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ ЭЛЕМЕНТОВ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Элемент модуля	**Форма контроля и оценивания**		
	Промежуточная аттестация	**Рубежный контроль**	**Текущий контроль**

МДК.02.01. Программные и программно-аппаратные средства защиты информации	Дифференцированный зачет (6 семестр), Курсовая работа (7 семестр), Экзамен (7 семестр)	Контрольная работа;	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Тестирование;
МДК.02.02 Криптографические средства защиты информации	Дифференцированный зачет (6 семестр)	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы;	Устные ответы; Формализованное наблюдение и оценка выполнения и защиты практической работы; Контроль выполнения самостоятельной работы; Оценка результатов выполнения контрольных работ;
УП. 02	Дифференцированный зачет (7 семестры)	------	Оценка результатов выполнения заданий и оформления отчетной документации по учебной практике
ПП 02	Дифференцированный зачет (8 семестр)	------	Оценка выполнения работ и оформления отчетной документации на производственной практике
Профессиональный модуль ПМ.02	Экзамен по модулю		

2.2. Общие/профессиональные компетенции, проверяемые дополнительно:

ОК	Основные показатели результата	Дополнительные формы контроля		
		Портфо-лио	Курсовое проектирование	Промежуточная аттестация по практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	выбранный способ решения задачи аргументирован; доказана оптимальность выбранного способа	-	+	-

	решения применительно к контексту тематики курсового проекта			
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	˜ наличие дипломов, грамот и сертификатов участия в мероприятиях по специальности; ˜ наличие дипломов, грамот и сертификатов участия в мероприятиях по формированию SoftSkills; ˜ положительный отзыв руководителя производственной практики.	+	-	+
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	˜ пояснительная записка оформлена грамотно на государственном языке; ˜ выдержан научный стиль изложения материала;	-	+	-
ОК 09. Использовать информационные технологии в профессиональной деятельности	˜ в процессе подготовки пояснительной записки эффективно использовались различные офисные приложения для обработки текстовой, числовой информации; ˜ защита курсового проекта осуществлялась с использованием презентационной графики.	-	+	-
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	˜ список литературы содержит источники как на русском, так и на иностранных языках.	-	+	-

3. ОЦЕНКА ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Вопросы для устного опроса по темам

Критерии оценки

«**Отлично**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«**Хорошо**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«**Удовлетворительно**» ставится, если:

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

«**Неудовлетворительно**» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах);
- знания отсутствуют, речь неграмотная

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

Тема 1.1 Предмет и задачи программно-аппаратной защиты информации.

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

Тема 1.2 Стандарты безопасности.

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

Тема 1.3 Защищенная автоматизированная система.

1. Автоматизация процесса обработки информации.
2. Понятие автоматизированной системы.

3. Особенности автоматизированных систем в защищенном исполнении.

4. Основные виды АС в защищенном исполнении.

5. Методы создания безопасных систем.

6. Методология проектирования гарантированно защищенных КС. 7. Дискреционные модели.

8. Мандатные модели.

Тема 1.4 Дестабилизирующее воздействие на объекты защиты.

1. Источники дестабилизирующего воздействия на объекты защиты.

2. Способы воздействия на информацию.

3. Причины и условия дестабилизирующего воздействия на информацию.

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

1. Понятие несанкционированного доступа к информации. 2. Основные подходы к защите информации от НСД.

3. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.

4. Доступ к данным со стороны процесса.

5. Особенности защиты данных от изменения. Шифрование.

Раздел 3. Защита информации в локальных сетях

Тема 3.1 Основы построения защищенных сетей.

1. Сети, работающие по технологии коммутации пакетов.

2. Стек протоколов TCP/IP. Особенности маршрутизации

3. Штатные средства защиты информации стека протоколов TCP/IP.

4. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

Тема 3.2 Средства организации VPN.

1. Виртуальная частная сеть. Функции, назначение, принцип построения.

2. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.

3. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки.

4. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.

Раздел 4. Защита информации в сетях общего доступа

Тема 4.1 Обеспечение безопасности межсетевого взаимодействия.

1. Методы защиты информации при работе в сетях общего доступа.

2. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.

3. Основные типы firewall. Симметричные и несимметричные firewall.

4. Уровень 1. Пакетные фильтры.

5. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.

6. Уровень 3. Proxy-сервера прикладного уровня.

7. Однохостовые и мультихостовые firewall.

8. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций.

9. Требования по сертификации межсетевых экранов.

Раздел 5. Защита информации в базах данных

Тема 5.1 Защита информации в базах данных.

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

Тема 5.2 Мониторинг систем защиты.

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

Тема 5.3 Изучение мер защиты информации в информационных системах.

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

Экзаменационные вопросы

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

Ботнеты. Принцип функционирования. Методы обнаружения.

20. Классификация антивирусных средств. Сигнатурный и эвристический анализ. 21. Защита от вирусов в "ручном режиме".

22. Основные концепции построения систем антивирусной защиты на предприятии.

23. Несанкционированное копирование программ как тип НСД.

24. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.

25. Защитные механизмы в современном программном обеспечении на примере MS Office.

26. Проблема защиты отчуждаемых компонентов ПЭВМ.

27. Методы защиты информации на отчуждаемых носителях. Шифрование.

28. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.

29. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов.

30. Безвозвратное удаление данных. Принципы и алгоритмы.

31. Устройства Touch Memory.

32. СОВ и СОА, отличия в функциях. Основные архитектуры СОВ.

33. Использование сетевых снифферов в качестве СОВ.

34. Аппаратный компонент СОВ. Программный компонент СОВ.

35. Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий.

36. Штатные средства защиты информации стека протоколов TCP/IP.

37. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

38. Виртуальная частная сеть. Функции, назначение, принцип построения. 39. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.

40. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности.

41. Основные типы firewall. Симметричные и несимметричные firewall.

42. Однохостовые и мультихостовые firewall.

43. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту, исходя из архитектуры и выполняемых функций.

44. Основные типы угроз. Модель нарушителя.

45. Средства идентификации и аутентификации. Управление доступом. 46. Средства контроля целостности информации в базах данных.

47. Средства аудита и контроля безопасности. Критерии защищенности баз данных.

48. Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации.

49. Классификация сетевых мониторов.

50. Системы управления событиями информационной безопасности (SIEM).

3.2. Контрольно-оценочные средства (КОС) для текущего контроля знаний, умений, обучающихся по МДК.02.02 Криптографические средства защиты информации

Вопросы для устного опроса по темам

Критерии оценки

«**Отлично**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний о материалах, технологиях изучения;
- доказательно раскрыты основные понятия, термины и др.;
- в ответе отслеживается четкая структура, выстроенная в логической последовательности;
- ответ изложен грамотным языком;
- на возникшие вопросы давались четкие, конкретные ответы, показывая умение выделять существенные и несущественные моменты материала.

«**Хорошо**» ставится, если:

- дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные моменты материала;
- ответ четко структурирован, выстроен в логической последовательности; - изложен грамотным языком;
- однако были допущены неточности в определении понятий, терминов и др.

«**Удовлетворительно**» ставится, если:

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

«**Неудовлетворительно**» ставится, если:

- дан неполный ответ на поставленный вопрос, логика и последовательность изложения имеют существенные нарушения;
- допущены существенные ошибки в теоретическом материале (понятиях, терминах);
- знания отсутствуют, речь неграмотная

Тема 1.1 Введение. Математические основы криптографии

7. Предмет и задачи криптографии. История криптографии. Основные термины.
8. Элементы теории множеств. Группы, кольца, поля.
9. Делимость чисел. Признаки делимости. Простые и составные числа.
10. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа.

Алгоритм Евклида для нахождения НОД.

11. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.
12. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма - Эйлера. Алгоритм быстрого возведения в степень по модулю.

Тема 2.1 Методы криптографической защиты информации.

4. Классификация основных методов криптографической защиты. Методы симметричного шифрования.
5. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.
6. Методы перестановки. Табличная перестановка, маршрутная перестановка.

Тема 2.2. Криптоанализ

1. Основные методы криптоанализа. Криптографические атаки.

Тема 2.3 Поточные шифры и генераторы псевдослучайных чисел

2. Основные принципы поточного шифрования

Тема 3.1 Кодирование информации. Компьютеризация шифрования

1. Кодирование информации. Символьное кодирование. Смысловое кодирование.

2. Компьютеризация шифрования. Аппаратное и программное шифрование.

Тема 3.2 Симметричные системы шифрования

1. Общие сведения. Структурная схема симметричных криптографических систем.

Тема 3.3 Асимметричные системы шифрования

1. Однонаправленные хеш-функции. Алгоритмы цифровой подписи

Тема 3.5 Алгоритмы обмена ключей и протоколы аутентификации

1. Задание для устного опроса по темам 1. Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация.

Тема 3.6 Криптозащита информации в сетях передачи данных

1. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр.

Тема 3.7 Защита информации в электронных платежных системах

1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.

Тема 3.8. Компьютерная стеганография.

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

Экзаменационные вопросы

1. Предмет и задачи криптографии. История криптографии. Основные термины. 2. Элементы теории множеств. Группы, кольца, поля.

3. Делимость чисел. Признаки делимости. Простые и составные числа.

4. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.

5. Отношения сравнимости. Свойства сравнений. Модулярная арифметика.

6. Классы. Полная и приведенная система вычетов. Функция Эйлера.

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

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

9. Китайская теорема об остатках.

10. Проверка чисел на простоту. Алгоритмы генерации простых чисел.

11. Метод пробных делений. Решето Эратосфена.

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

13. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.

14. Арифметические операции над большими числами.

15. Эллиптические кривые и их приложения в криптографии.

16. Классификация основных методов криптографической защиты. Методы симметричного шифрования

17. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.

18. Методы перестановки. Табличная перестановка, маршрутная перестановка 19. Гаммирование. Гаммирование с конечной и бесконечной гаммами

20. Основные методы криптоанализа. Криптографические атаки.

21. Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса.

22. Перспективные направления криптоанализа, квантовый криптоанализ.

23. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.

24. Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.

25. Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII.

26 Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств.

27. Общие сведения. Структурная схема симметричных криптографических систем 28. Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.

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

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

31. Элементы теории чисел в криптографии с открытым ключом.

32. Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи

33. Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации.

34. Взаимная аутентификация. Односторонняя аутентификация

35. Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей.

36. Криптомаршрутизатор. Пакетный фильтр

37. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.

38. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер

39. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.

40. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.

41. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ

4. Требования к дифференцированному зачету по учебной и (или) производственной практике

Дифференцированный зачет по учебной и (или) производственной практике выставляется с учетом данных аттестационного листа (характеристики профессиональной деятельности обучающегося/студента на практике) с указанием видов работ, выполненных обучающимся во время практики, их объема, качества выполнения в соответствии с технологией и (или) требованиями организации, в которой проходила практика.

4.1. Оценочные материалы

Перечень вопросов к собеседованию по производственной практике

1. Краткая характеристика места практики
2. Требования по защите персональных данных
3. Требования по защите конфиденциальных данных предприятия 4. Системы контроля и управления доступом на предприятии
5. Способы ограничения доступа к информации

6. Признаки наличия вредоносного программного обеспечения 7. Средства защиты информации в компьютерных сетях

8. Средства обнаружения компьютерных атак

9. Способы предупреждения компьютерных атак

10. Программно-аппаратные средства уничтожения информации и носителей информации.

5. Комплект экзаменационных материалов

Задания для экзаменующегося

Задание 1

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

3. 5., ПК 2.6.

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

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

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

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

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

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно- аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Инструкция

Внимательно прочитайте задание. Время выполнения задания – 40 минут Текст задания:

Вариант № 1

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

Вариант № 2

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

Вариант № 3

Опишите технологию создания и управления учетными записями пользователей. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного

пользователя. Проделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

Вариант № 4

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

Вариант № 5

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

Вариант № 6

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

Вариант № 7

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

Вариант № 8

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

Вариант № 9

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

Вариант № 10

Создайте новую книгу для проведения простых вычислений суммы, разности, произведения над числами, удовлетворяющими некоторому условию, на основе данных, вводимых пользователем. Задайте проверку выполнения условия (например, только положительные, только отрицательные, только целые из определенного диапазона значений и т.п.) для ячеек, в которые будет осуществляться ввод данных. Установите защиту: ячейки для ввода данных должны быть разблокированы, остальное содержимое листа – защищено от изменений; формулы, по которым производятся вычисления, – скрыты. При установке защиты листа разрешить всем пользователям настраивать ширину столбцов и высоту строк, менять заливку ячеек.

ЗАДАНИЕ 2

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

ОК 09, ОК 10

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

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

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

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном

языке.

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания – 40 минут

Вариант 1.

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

Вариант 2.

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

Вариант 3.

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

Вариант 4.

Представьте алгоритм работы российского стандарта шифрования ГОСТ 2 8 1 4 7 - 8 9 . Выполнить ручное шифрование исходного текста с помощью алгоритма ГОСТ 28147-89. Сравните алгоритмы шифрования ГОСТ 28147-89 и DES. Приведите примеры программ симметричного шифрования.

Вариант 5.

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

Вариант 6.

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

Вариант 7.

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

Вариант 8.

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

Вариант 9.

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

Вариант 10.

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

ЗАДАНИЕ 3

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

ОК 09, ОК 10

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

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

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

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

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

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

Инструкция

Внимательно прочитайте задание.

Вы можете воспользоваться ПК и необходимым программным обеспечением для выполнения задания

Время выполнения задания – 40 минут

Вариант 1.

Напишите краткое руководство по основным командам Linux для начинающих пользователей.

Включите примеры использования каждой команды.

Вариант 2.

Исследуйте и сравните три популярных дистрибутива Linux (например, Ubuntu, Fedora и CentOS). Опишите их основные особенности и целевую аудиторию.

Вариант 3.

Установите GRUB на виртуальную машину с Linux. Опишите процесс установки и настройки, а также как добавить новые записи в меню загрузки.

Вариант 4.

Опишите, что такое демоны в Linux. Приведите примеры распространенных демонов и их функций в системе.

Вариант 5.

Напишите сценарий на Bash, который будет отслеживать и выводить информацию о текущих процессах в системе (например, используя команды ps, top и htop).

Вариант 6.

Объясните, как работает файловая система в Linux. Опишите, как создать и отформатировать новый раздел с помощью командной строки.

Вариант 7.

Установите VirtualBox на свою машину и создайте виртуальную машину с Ubuntu. Опишите

процесс установки и настройки параметров виртуальной машины.

Вариант 8.

Установите Debian 11 Desktop на виртуальную машину. Опишите процесс установки, включая выбор пакетов и конфигурацию сети.

Вариант 9.

Напишите краткое руководство по использованию текстовых редакторов Vim и Nano. Включите основные команды для редактирования, сохранения и выхода из редакторов.

Вариант 10.

Используя инструменты командной строки, такие как top, htop и ps, создайте отчет о текущих процессах на вашей системе. Опишите, как интерпретировать полученные данные.

5.1. Пакет экзаменатора

Условия выполнения задания:

Инструкция

Ознакомьтесь с заданиями для экзаменующихся

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

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

Задание № 1–40 минут

Задание № 2–40 минут

Задание № 3–40 минут

Всего на экзамен – 2 часа

Экзамен проводится в группе в количестве - 19 человек

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

5.2. Критерии оценки

Показатель	Результат	Оценка

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

Параметры оценивания:

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