Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Колледж информатики и программирования

СОГЛАСОВАНО
Акционерное общество
«Особое Конструкторское Бюро Систем
Автоматизированного Проектирования»
(АО «ОКБ САПР»)
Генеральный директор

_____ И.Г. Назаров
«28» июня 2023 г.

УТВЕРЖДАЮ

Заместитель директора
по учебной работе

_____ Н.Ю. Долгова
«26» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Москва 2023 г.

Рабочая программа учебный дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчики:
Поколодина Е.В., к.э.н., доцент, преподаватель высшей квалификационной категории Колледжа информатики и программирования.
Рой А.В., к.т.н., преподаватель высшей квалификационной категории Колледжа информатики и программирования.
Мурашкин О.Н., заведующий лабораторией Колледжа информатики и программирования.

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии Основы информационной безопасности

Протокол от «11» мая 2023 г. № 9

Председатель предметной (цикловой) комиссии _____ А.Л. Маринич

1. Общая характеристика рабочей программы профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Общие компетенции
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 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, применять стандарты антикоррупционного поведения.
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 языках.
ОК.11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.2. Перечень профессиональных компетенций

Код	Профессиональные компетенции
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 студент должен:

иметь практический опыт	– 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*, информирование персонала об угрозах безопасности информации*;* – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе; – *применения технологии фильтрации различных видов трафика*; * – *осуществлять фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.**
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, *проводить мониторинг, анализ и сравнение*

	эффективности программно-аппаратных средств защиты информации в операционных системах; – 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; *- оформлять эксплуатационную документацию программно аппаратных средств защиты информации;** *- определять цели и задачи в изучении проекта;** *-разрабатывать политику информационной безопасности на основе самостоятельной классификации объектов защиты;* – *осуществлять установку, развёртывание, настройку и использованием DLP-систем.**
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*, общие принципы функционирования средств защиты информации, в том числе и криптографической 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. – *теоретические основы корпоративной защиты информации от внутренних ИТ-угроз;** – *методику проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; современные стандарты и средства корпоративной защиты. **

**вариативная часть*

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов 836, в том числе в форме практической подготовки 500 часа.

Из них на освоение МДК 536 час.

в том числе самостоятельная работа 20 час.

Практики, в том числе учебная 144 час.

производственная (по профилю специальности) 144 час.

Экзамен по модулю 12 час.

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак.час.						
				Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа
				Обучение по МДК				Практики		
				Всего	*В том числе*			Учебная	Производственная	
					Промежуточная аттестация	лабораторных и практических занятий	курсовых работ (проектов)			
1	2	3		4		5	6	7	8	10
ПК 2.1 – ПК 2.6 ОК 01-ОК 11	**Раздел 1.** Применение программных и программно-аппаратных средств защиты информации	328	172	232	18	70	30	72	-	6
ПК 2.4 ОК 01-ОК 11	**Раздел 2.** Криптографические средства защиты информации	216	104	156	18	68	-	36	-	6
ПК 2.1 – ПК 2.4, ПК 2.6 ОК 01-ОК 11	**Раздел 3.** Корпоративная защита от внутренних угроз информационной безопасности	136	80	92		44	-	36	-	8

ПК 2.1 – ПК 2.6 ОК 01-ОК 11	Производственная практика (по профилю специальности)	144	144						144	
	Экзамен по модулю	12			12					
	Всего:	836	500	480	48	182	30	144	144	20

2.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа студентов, курсовой проект (работа)	Объем часов
1	2	3
Раздел 1 ПМ.02. Применение программных и программно-аппаратных средств защиты информации		**328**
МДК.02.01. Программные и программно-аппаратные средства защиты информации		**256**
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		**44**
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	Содержание	6
	1.Предмет и задачи программно-аппаратной защиты информации	6
	2.Основные понятия программно-аппаратной защиты информации	
	3.Классификация методов и средств программно-аппаратной защиты информации	
	В том числе практических и лабораторных занятий	-
Тема 1.2. Стандарты безопасности	Содержание	10
	1.Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	4
	2.Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	
	В том числе практических и лабораторных занятий	6
	1. Практическое занятие «Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов».	4
	2. Практическое занятие «Обзор стандартов. Работа с содержанием стандартов»	2

Тема 1.3. Защищенная автоматизированная система	Содержание	10
	1.Автоматизация процесса обработки информации	4
	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	
	В том числе практических и лабораторных занятий	6
	1. Практическое занятие «Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему.Идентификация и аутентификация пользователей. Разграничение доступа».	2
	2. Практическое занятие «Регистрация событий (аудит). Контроль целостности данных»	2
	3. Практическое занятие «Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности»	2
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	Содержание	8
	1.Источники дестабилизирующего воздействия на объекты защиты	4
	2.Способы воздействия на информацию	
	3.Причины и условия дестабилизирующего воздействия на информацию	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Распределение каналов в соответствии с источниками воздействия на информацию»	4
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	Содержание	10
	1.Понятие несанкционированного доступа к информации	6
	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.	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Организация доступа к файлам»	2
	2. Практическое занятие «Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД»	2
Раздел 2. Защита автономных автоматизированных систем		**54**
Тема 2.1. Основы защиты автономных автоматизированных систем	Содержание	6
	1.Работа автономной АС в защищенном режиме	6
	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.	
	В том числе практических и лабораторных занятий	-
Тема 2.2. Защита программ от изучения	Содержание	6
	1.Изучение и обратное проектирование ПО	6
	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.	
	В том числе практических и лабораторных занятий	-
Тема 2.3. Вредоносное программное обеспечение	Содержание	8
	1.Вредоносное программное обеспечение как особый вид разрушающих воздействий	6
	2.Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	
	3.Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	

	4.Бот-неты. Принцип функционирования. Методы обнаружения	
	5.Классификация антивирусных средств. Сигнатурный и эвристический анализ	
	6.Защита от вирусов в "ручном режиме"	
	7.Основные концепции построения систем антивирусной защиты на предприятии	
	В том числе практических и лабораторных занятий	2
	1. Практическое занятие «Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО»	2
Тема 2.4. Защита программ и данных от несанкционированного копирования	Содержание	8
	1.Несанкционированное копирование программ как тип НСД	4
	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	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Защита информации от несанкционированного копирования с использованием специализированных программных средств»	2
	2. Практическое занятие «Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)»	2
Тема 2.5. Защита информации на машинных носителях	Содержание	14
	1.Проблема защиты отчуждаемых компонентов ПЭВМ.	6
	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.	
	В том числе практических и лабораторных занятий	8
	1. Практическое занятие «Применение средства восстановления остаточной информации на примере Foremost или аналога»	2
	2. Практическое занятие «Применение специализированного программного средства для восстановления удаленных файлов»	2

	3. Практическое занятие «Применение программ для безвозвратного удаления данных»	2
	4. Практическое занятие «Применение программ для шифрования данных на съемных носителях»	2
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	Содержание	4
	1.Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	4
	2.Устройства Touch Memory	
	В том числе практических и лабораторных занятий	-
Тема 2.7. Системы обнаружения атак и вторжений	Содержание	8
	1.СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	4
	2.Использование сетевых снифферов в качестве СОВ	
	3.Аппаратный компонент СОВ	
	4.Программный компонент СОВ	
	5.Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений»	4
Раздел 3. Защита информации в локальных сетях		**12**
Тема 3.1. Основы построения защищенных сетей	Содержание	4
	1.Сети, работающие по технологии коммутации пакетов	4
	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.	
	В том числе практических и лабораторных занятий	-
Тема 3.2. Средства организации VPN	Содержание	8
	1.Виртуальная частная сеть. Функции, назначение, принцип построения	4
	2.Криптографические и некриптографические средства организации VPN	

	3.Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	
	4.Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	5.Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Развертывание VPN»	4
Промежуточная аттестация в форме дифференцированного зачета по МДК.02.01		**2**
Раздел 4. Защита информации в сетях общего доступа		**12**
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	Содержание	12
	1.Методы защиты информации при работе в сетях общего доступа.	8
	2.Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности	
	3.Дифференцированный зачет	
	4.Основные типы firewall. Симметричные и несимметричные firewall.	
	5.Уровень 1. Пакетные фильтры	
	6.Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	7.Уровень 3. Proxy-сервера прикладного уровня	
	8.Однохостовые и мультихостовые firewall.	
	9.Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	
	10.Требования по сертификации межсетевых экранов	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr».	2
	2. Практическое занятие «Изучение различных способов закрытия "опасных" портов»	2
Раздел 5. Защита информации в базах данных		**10**
Тема 5.1. Защита информации в базах данных	Содержание	10
	1.Основные типы угроз. Модель нарушителя	6
	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	

	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Изучение механизмов защиты СУБД MS Access»	2
	2. Практическое занятие «Изучение штатных средств защиты СУБД MSSQL Server»	2
Раздел 6. Мониторинг систем защиты		**68**
Тема 6.1. Мониторинг систем защиты	Содержание	8
	1.Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	6
	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). Обзор SIEM-систем на мировом и российском рынке.	
	В том числе практических и лабораторных занятий	2
	1. Практическое занятие «Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов. Проведение аудита ЛВС сетевым сканером (на примере MaxPatrol 8)»	2
Тема 6.2. Изучение мер защиты информации в информационных системах	Содержание	4
	1.Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2
	В том числе практических и лабораторных занятий	2
	Практическое занятие «Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке».	2
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Содержание	8
	Не предусмотрено	-
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов»	2

	Практическое занятие «Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов»	2
	Практическое занятие «Изучение типовых решений для построения VPN на примере VipNet или других аналогов»	2
	Практическое занятие «Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов»	1
	Практическое занятие «Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов»	1
Тема 6.4 *Изучение программно-аппаратных средств защиты информации ОКБ САПР**	Содержание	48
	1.Платформенные решения ОКБ САПР	40
	2.Доверенная загрузка на базе Аккорд-АМДЗ	
	3.Интеграция СЗИ НСД с контролем доступа и видеонаблюдением	
	4.Применение ПАК Аккорд для разграничения доступа к данным	
	5.Программно-аппаратный журнал 6 ПАК «МНЛ»	
	7.Работа с системой управления событиями информационной безопасности (MaxPatrol SIEM).	
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Установка и настройка прав пользователя и администратора в АМДЗ Аккорд GX . Изучение особенностей защитных функций АМДЗ Аккорд GX»	2
	Практическое занятие «Работа с защищенным служебным носителем ОКБ САПР Секрет Особого назначения. Установка и настройка политик».	2
	Практическое занятие «Работа с защищенным служебным носителем ОКБ САПР Секрет Особого назначения. Изучение особенностей работы с защищенным сектором накопителя Секрет Особого назначения»	2
	Практическое занятие «Работа с защищенным служебным носителем ОКБ САПР Секрет Особого назначения»	2
Примерная тематика внеаудиторной самостоятельной работы, реферат на темы: Изучение новых технологий хранения информации; Статистика и анализ крупных утечек информации за год; Поиск информации о новых видах атак на информационную систему;		6

Обзор современных программных и программно-аппаратных средств защиты; Сравнительный анализ современных программных и программно-аппаратных средств защиты; Проблемы работы корпоративных АИС в условиях удаленного доступа.	
Тематика курсовых проектов (работ) 1.Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 2.Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 3.Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) 4.Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) 5.Проблема защиты информации в облачных хранилищах данных и ЦОДах 6.Защита сред виртуализации	**30**
Консультации	**6**
Промежуточная аттестация в форме экзамена по МДК.02.01	**12**
Учебная практика раздела 1 Виды работ Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности Составление документации по учету, обработке, хранению и передаче конфиденциальной информации Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. Устранение замечаний по результатам проверки Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов. Применение математических методов для оценки качества и выбора наилучшего программного средства Проведение аудита информационной безопасности	**72**

*Применение ОС Kali Linux для тестирования информационной системы на проникновение** *Установка и настройка ОС Astra Linux**		
Раздел 2 ПМ.02. Применение криптографических средств защиты информации		**216**
МДК.02.02. Криптографические средства защиты информации		**180**
Введение	Содержание	2
	1.Предмет и задачи криптографии. История криптографии. Основные термины	2
	В том числе практических и лабораторных занятий	-
Раздел 1. Математические основы защиты информации		**30**
Тема 1.1. Математические основы криптографии	Содержание	30
	1.Элементы теории множеств. Группы, кольца, поля.	24
	2.Делимость чисел. Признаки делимости. Простые и составные числа.	
	3.Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	
	4.Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	
	5.Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю.	
	6.Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	
	7.Китайская теорема об остатках.	
	8.Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	
	9.Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	
	10.Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	
	11.Арифметические операции над большими числами.	
	12.Эллиптические кривые и их приложения в криптографии.	
	В том числе практических и лабораторных занятий	6
	Практическое занятие «Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений»	2
	Практическое занятие « Проверка чисел на простоту»	2

	Практическое занятие «Решение задач с элементами теории чисел».	2
Раздел 2. Классическая криптография		**36**
Тема 2.1. Методы криптографического защиты информации	Содержание	14
	1.Классификация основных методов криптографической защиты. Методы симметричного шифрования	8
	2.Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	
	3.Методы перестановки. Табличная перестановка, маршрутная перестановка	
	4.Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	В том числе практических и лабораторных занятий	6
	Практическое занятие «Применение классических шифров замены»	2
	Практическое занятие «Применение классических шифров перестановки»	2
	Практическое занятие «Применение метода гаммирования»	2
Тема 2.2. Криптоанализ	Содержание	16
	1.Основные методы криптоанализа. Криптографические атаки.	6
	2.Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	
	3.Перспективные направления криптоанализа, квантовый криптоанализ.	
	В том числе практических и лабораторных занятий	10
	Практическое занятие «Криптоанализ шифра простой замены методом анализа частотности символов»	4
	Практическое занятие «Криптоанализ классических шифров методом полного перебора ключей»	2
	3. Практическое занятие «Криптоанализ шифра Вижинера»	4
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел (ПСЧ)	Содержание	6
	1.Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	4
	2.Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	
	В том числе практических и лабораторных занятий	2
	Практическое занятие «Применение методов генерации ПСЧ»	2
Раздел 3. Современная криптография		**88**

Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Содержание	14
	1.Кодирование информации. Символьное кодирование. Смысловое кодирование.	6
	2.Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	
	3.Компьютеризация шифрования. Аппаратное и программное шифрование	
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Кодирование информации»	2
	Практическое занятие «Программная реализация классических шифров»	2
	Практическое занятие «Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге».	2
	Практическое занятие «Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств»	2
Тема 3.2. Симметричные системы шифрования	Содержание	24
	1.Общие сведения. Структурная схема симметричных криптографических систем.	14
	2.Изучение зарубежных симметричных шифров DES и AES. Современные методы криптоанализа симметричных шифров*	
	3.Отечественные стандарты шифрования ГОСТ 28147-89*	
	4.Отечественные стандарты шифрования ГОСТ 28147-89, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 и их криптоанализ	
	В том числе практических и лабораторных занятий	10
	Практическое занятие «Программная реализация симметричных криптографических алгоритмов DES, AES»	2
	Практическое занятие «*Программная реализация симметричных криптографических алгоритмов RC»**	2
	Практическое занятие «*Программная реализация симметричных криптографических алгоритмов отечественного стандартов ГОСТ 28147-89»**	2
	Практическое занятие *«Программная реализация симметричных криптографических алгоритмов отечественного стандартов ГОСТ Р 34.13-2015»**	2
	Практическое занятие «*Программная реализация симметричных криптографических алгоритмов отечественного стандартов ГОСТ Р 34.13-2015»**	2

Тема 3.3. Асимметричные системы шифрования	Содержание	8
	1.Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом.	4
	2.Элементы теории чисел в криптографии с открытым ключом.	
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие в форме практической подготовки Применение различных асимметричных алгоритмов.	2
	2. Практическое занятие в форме практической подготовки Изучение программной реализации асимметричного алгоритма RSA	2
Тема 3.4. Аутентификация данных. Электронная подпись	Содержание	12
	1.Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	4
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Применение различных функций хеширования, анализ особенностей хешей»	2
	Практическое занятие «Применение криптографических атак на хеш-функции2.	4
	Практическое занятие «Изучение программно-аппаратных средств, реализующих основные функции ЭП»	2
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	Содержание	10
	1.Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	4
	В том числе практических и лабораторных занятий	6
	Практическое занятие «Применение протокола Диффи-Хеллмана для обмена ключами шифрования».	2
	Практическое занятие «Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos».	4
Тема 3.6. Криптозащита информации в сетях передачи данных	Содержание	4
	1.Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр	4
	2.Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	

	В том числе практических и лабораторных занятий	-
Тема 3.7. Защита информации в электронных платежных системах	Содержание	8
	1.Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер	6
	2.Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	
	В том числе практических и лабораторных занятий	2
	Практическое занятие «Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей»	2
Тема 3.8. Компьютерная стеганография	Содержание	8
	1.Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	2
	2.Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	
	В том числе практических и лабораторных занятий	6
	Практическое занятие «Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ»	4
	Практическое занятие «Реализация простейших стеганографических алгоритмов»	2
Примерная тематика внеаудиторной самостоятельной работы, реферат на темы: Оптимизация методов частотного анализа моноалфавитных шифров; Анализ современных симметричных криптоалгоритмов; Анализ современных асимметричных криптоалгоритмов; Перспективные направления криптографии.		6
Консультации		**6**
Промежуточная аттестация в форме экзамена по МДК.02.02		**12**
Учебная практика раздела 2 Виды работ Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи *Исследование алгоритмов современных зарубежных симметричного шифров FEAL, IDEA, RC4, RC5, RC6. Их программная реализация и современные методы криптоанализа**		**36**

*Исследование алгоритмов современных отечественных симметричного шифров Магма и Кузнечик. Их программная реализация и современные методы криптоанализа** *Исследование алгоритмов хэширования MD4, MD5, SHA-1, SHA-2 и SHA-256. Применение функций хэширования в ЭЦП и аутентификации сообщений на примере Kerberos** *Изучение квантовых методов в криптографии. Квантовые методы криптоанализа и программная реализация квантовых алгоритмов на примере алгоритма факторизации Шора**		
Раздел модуля 3. *Корпоративная защита от внутренних угроз информационной безопасности* *		**136**
МДК 02.03 Корпоративная защита от внутренних угроз информационной безопасности*		**100**
Тема 1.1. Теоретические основы корпоративной защиты от внутренних угроз	Содержание	12
	1.Системы DLP и требования по информационной безопасности. Назначение и отличия DLP систем.	8
	2.Классификация нарушителей и угроз корпоративной информационной безопасности. Особенности оценки ущерба.	
	3. Исследование структуры информационных потоков предприятия	
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Формальное описание информационных потоков»	2
	Практическое занятие «Формирование моделей потенциальных внутренних нарушителей и угроз»	2
Тема 1.2. Нормативно – правовые и административно – организационные аспекты корпоративной защиты от внутренних угроз	Содержание	30
	1. Нормативно – правовые акты и аспекты корпоративной защиты информации. Классификация информации «Государственная тайна». Ответственность за нарушение.	12
	2.Обзор практики применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности.	
	3. Формирование процессов и процедур аудита информационной безопасности. Обследование корпоративных информационных систем. Состояние корпоративной информации.	
	В том числе практических и лабораторных занятий	18
	Практическое занятие «Проведение анализа данных об организационной и функциональной структуре информационной системы предприятия»	4
	Практическое занятие «Формирование заключение на соответствие/не соответствие заданным критериям. Формирование рекомендаций для повышения уровня надежности и безопасности информационной системы предприятия»	4

	Практическое занятие «Методика разработки политик и правил безопасности для перекрытия канала передачи (утечки) данных с занесением в DLP – систему»	4
	Практическое занятие «Разработка объектов защиты, категорий, технологий защиты в DLP – системе»	6
Тема 1.3. Защита корпоративной информации с использованием автоматизированных систем контроля информационных потоков	Содержание	48
	1.Системы контроля информационных потоков/ Контролируемые каналы передачи данных	26
	2.Назначение системы IW Trafic monitor / Архитектура продукта IW Trafic monitor	
	3.Технологии анализа детектируемых объектов/ Задачи и принципы работы дополнительных модулей системы IW Device Monitor и IW Crawler	
	4. Изучение интерфейса IW Device Monitor	
	5.Поиск инцидентов.	
	В том числе практических и лабораторных занятий	22
	Практическое занятие «Изучение интерфейса IW Device Monitor управления системы корпоративной защиты информации на рабочих станциях «	2
	Практическое занятие «Создание политик и правил информационной безопасности в системе IW Device Monitor. Поиск инцидентов».	6
	Практическое занятие «Изучение интерфейса управления системы корпоративной защиты информации IW Trafic monitor»	4
	Практическое занятие «Создание политик информационной безопасности в системе IW Trafic monitor. Поиск инцидентов».	6
	Практическое занятие «Анализ и контроль общедоступных сетевых ресурсов с помощью системы IW Crawler»	4
Примерная тематика внеаудиторной самостоятельной работы Принцип построения регулярных выражений при написании технологии запросов. Отличия в синтаксисе написания обычных «регулярок» и для DLP-систем. «Корпоративная защита от внутренних угроз»		8
Промежуточная аттестация в форме дифференцированного зачета по МДК 02.03		**2**
Учебная практика раздела 3 Виды работ Проведение всего комплекса технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его; Проведение всего цикла работ по установке, развёртыванию, настройке, использованию DLP-систем;		**36**

Разработка политик информационной безопасности; Применение технологий фильтрации различных видов трафика; Фильтрация перехваченного трафика для поиска найденных инцидентов; Анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности; Диагностика работоспособности системы; Подготовка отчета о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой); Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.	
Производственная практика Виды работ Анализ принципов построения систем информационной защиты производственных подразделений; Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы; Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении; Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации; Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики; *Администрирование автоматизированных технических средств управления и контроля информации и информационных потоков** *Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом** *Выявление потоков передачи данных и возможных каналов утечки информации** *Использование механизмов создания фильтров для анализа перехваченного трафика и выявленных инцидентов** *Проведение детектирования атак (потенциальных угроз) в ручном, автоматизированном и автоматическом режиме. **	**144**
Экзамен по профессиональному модулю	**12**
Всего	**836**

3. Условия реализации рабочей программы профессионального модуля

3.1. Для реализации программы профессионального модуля предусмотрена следующие специальные помещения:

учебных кабинетов – нормативного правового обеспечения информационной безопасности, кабинет информатики; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

3.2. Информационное обеспечение реализации программы

Основные печатные и электронные издания:

1. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

2. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844

4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242

5. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. —

Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

6. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

Дополнительные источники

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2009 г
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены

приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки

безопасности информационных технологий. Часть 2. Функциональные требования безопасности

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

36. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

38. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005.

39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

40. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

41. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

42. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

43. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

44. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

46. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

47. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

48. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

51. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

4. Контроль и оценка результатов освоения профессионального модуля

Код и наименование общих и профессиональных компетенций формируемых в рамках модуля	Критерии оценки	Формы и методы контроля, в том числе по учебной и производственной практике
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экзамен по модулю, экспертное наблюдение выполнения лабораторных занятий, экспертное наблюдение выполнения практических занятий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экзамен по модулю, результаты защиты курсового проекта, экспертное наблюдение выполнения лабораторных занятий, экспертное наблюдение выполнения практических занятий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экзамен, экзамен по модулю, экспертное наблюдение выполнения лабораторных занятий, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экзамен по модулю, результаты защиты курсового проекта, экспертное наблюдение выполнения лабораторных занятий, экспертное наблюдение выполнения практических занятий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, диф.зачет, экзамен по модулю, результаты защиты курсового проекта, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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.	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, диф.зачет, экзамен по модулю, результаты защиты курсового проекта, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Код и наименование общих и профессиональных компетенций формируемых в рамках модуля	Критерии оценки	Формы и методы контроля, в том числе по учебной и производственной практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- выбор метода и способа решения профессиональных задач с соблюдением техники безопасности и согласно заданной ситуации; -оценка эффективности и качества выполнения согласно заданной ситуации	Наблюдение, мониторинг, оценка содержания портфолио студента.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- эффективный поиск необходимой информации; - информация, подобранная из разных источников в соответствии с заданной ситуацией	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 03. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- решение стандартных и нестандартных профессиональных задач в области эксплуатации компонент подсистем безопасности автоматизированных систем;	Мониторинг и рейтинг выполнения работ на учебной и производственной практике
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией; - демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями.	Подготовка рефератов, докладов, сообщений, использование электронных источников
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- - демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией; - демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями.	Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях.

Код и наименование общих и профессиональных компетенций формируемых в рамках модуля	Критерии оценки	Формы и методы контроля, в том числе по учебной и производственной практике
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- демонстрация интереса к будущей профессии; - демонстрация целеустремленности, самообразования и саморазвития	Наблюдение за ролью обучающегося в группе; портфолио
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- демонстрация качества принятых организационных решений - готовность к частой смене технологий в профессиональной деятельности; - анализ инноваций в области профессиональной деятельности.	Деловые игры - моделирование социальных и профессиональных ситуаций.
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- оценка собственного продвижения, личностного развития.	Контроль графика выполнения индивидуальной самостоятельной работы обучающегося; открытые защиты творческих и проектных работ
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- использование основных видов современной вычислительной техники; - эксплуатация и устранение типичных выявленных дефектов технических средств информатизации; - демонстрация результативной деятельности в области эксплуатации и технического сопровождения автоматизированных систем	Семинары учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады.

Код и наименование общих и профессиональных компетенций формируемых в рамках модуля	Критерии оценки	Формы и методы контроля, в том числе по учебной и производственной практике
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- использование основных видов современной вычислительной техники; - эксплуатация и устранение типичных выявленных дефектов технических средств информатизации; - демонстрация результативной деятельности в области эксплуатации и технического сопровождения автоматизированных систем	Семинары учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций.
ОК.11 Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- эффективный поиск и применение знаний финансовой грамотности; - информация, подобранная из разных источников в соответствии с заданной ситуацией	Семинары учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций