НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО
ученым педагогическим советом
(протокол №06-23 от «26» июня 2023 г.)
Председатель педагогического совета
Директор _____ Л.Н. Цой

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ДИСЦИПЛИНЫ

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

ППССЗ по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Объем дисциплины – 720 часов.

Якутск, 2023

Рабочая программа учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Укрупненная группа специальностей 10.00.00 Информационная безопасность.

Разработчики рабочей программы:	НПОУ «ЯКИТ»	Преподаватель	Михайлов И.И.
	(место работы)	(должность)	(инициалы, фамилия)

Обсуждено на заседании отделения «19» июня 2022 г. протокол №9/1

Председатель отделения Зав. отделения _____ И.В. Пронин

Рассмотрено на заседании методического совета «20» июня 2023 г. протокол №6

Председатель методического совета Заместитель директора по учебно-методической работе _____ «20» июня 2023 г.

Заместитель директора по учебно-методической работе _____ С.И. Томская «26» июня 2023 г.

№ п/п	Прилагаемый к Рабочей программе документ, содержащий текст обновления	Решение отделения		Подпись заведующего отделения	Фамилия И.О. заведующего отделения
		дата	Протокол №		
1.	Приложение № 1				
2.	Приложение № 2				
3.	Приложение № 3				
4.	Приложение № 4				
5.	Приложение № 5				

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОГО ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1.В результате изучения профессионального модуля студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему 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.

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.

ДПК 5.3. Разработка процедуры проверки работоспособности программного обеспечения

ДПК 5.4. Языки, утилиты и среды программирования, и средства пакетного выполнения процедур

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;

-работы с подсистемами регистрации событий;

-выявления событий и инцидентов безопасности в автоматизированной системе.

должен 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.

должен 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.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 720 часов, из них

на освоение МДК – 452 часов, в том числе

на промежуточную аттестацию по МДК – 6 часов,

на практики – 180 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОГО ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 2.1 – ПК 2.6 ОК 1-ОК 10	Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации	294	266	150	–	18	144	28
ПК 2.4 ОК 1-ОК 10	Раздел 2 модуля. Применение криптографических средств защиты информации	240	186	112	–	18	–	54
	Учебная практика	36	–	–	–	–	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	144					–	–
	Промежуточная аттестация	6	–	–	–	–	–	–

	Экзамен по профессиональному модулю	-	-	–	–	–	–	–
	Всего:	720	452	262	–	36	144	82

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		294	
МДК.02.01. Программные и программно-аппаратные средства защиты информации		266	
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации			
Тема 1. Предмет и задачи программно-аппаратной защиты информации	Предмет и задачи программно-аппаратной защиты информации Основные понятия программно-аппаратной защиты информации Классификация методов и средств программно-аппаратной защиты информации	5	
Тема 2. Стандарты безопасности	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) Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	5	
	Практические занятия 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	10	

	правовых актов. Обзор стандартов. Работа с содержанием стандартов		
Тема 3. Защищенная автоматизированная система	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем Методология проектирования гарантированно защищенных КС Дискреционные модели Мандатные модели	4	
	Практическое занятие Учет, обработка, хранение и передача информации в АИС Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей Разграничение доступа Регистрация событий (аудит). Управление политикой безопасности. Шаблоны безопасности Уничтожение остаточной информации. Контроль целостности данных	5	
Тема 4. Дестабилизирующее воздействие на объекты защиты	Источники дестабилизирующего воздействия на объекты защиты Способы воздействия на информацию Причины и условия дестабилизирующего воздействия на информацию Тематика практических занятий и лабораторных работ Распределение каналов в соответствии с источниками воздействия на информацию	4	
	Практические занятия Распределение каналов в соответствии с источниками воздействия на информацию.	2	
Тема 5. Принципы программно-аппаратной защиты информации от несанкционированного доступа организации	Понятие несанкционированного доступа к информации Основные подходы к защите информации от НСД Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам Доступ к данным со стороны процесса Особенности защиты данных от	4	

	изменения. Шифрование.		
	Практические занятия Организация доступа к файлам Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2	
Раздел 2. Защита автономных автоматизированных систем		51	
Тема 1. Основы защиты автономных автоматизированных систем	Работа автономной АС в защищенном режиме Алгоритм загрузки ОС. Штатные средства замыкания среды Расширение BIOS как средство замыкания программной среды Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка) Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	5	
Тема 2. Защита программ от изучения	Изучение и обратное проектирование ПО Способы изучения ПО: статическое и динамическое изучение Задачи защиты от изучения и способы их решения Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям.	4	
Тема 3. Вредоносное программное обеспечение	Вредоносное программное обеспечение как особый вид разрушающих воздействий Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Бот-неты. Принцип функционирования. Методы обнаружения Классификация антивирусных средств. Сигнатурный и эвристический анализ Защита от вирусов в "ручном режиме"	8	

	Основные концепции построения систем антивирусной защиты на предприятии		
	Практические занятия Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2	
Промежуточная аттестация по МДК.02.01			
Тема 4. Защита программ и данных от несанкционированного копирования	Несанкционированное копирование программ как тип НСД Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. Привязка ПО к аппаратному окружению и носителям Защитные механизмы в современном программном обеспечении на примере MS Office Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	6	
	Практическое занятие Защита информации от несанкционированного копирования с использованием специализированных программных средств Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	4	
Тема 5. Защита информации на машинных носителях	Проблема защиты отчуждаемых компонентов ПЭВМ Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	8	
	Практическое занятие Применение средства восстановления остаточной информации на примере Foremost или аналога Применение специализированного	4	

	программно средства для восстановления удаленных файлов Применение программ для безвозвратного удаления данных Применение программ для шифрования данных на съемных носителях		
Тема 6. Аппаратные средства идентификации и аутентификации пользователей	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ Устройства Touch Memory	4	
Тема 7. Системы обнаружения атак и вторжений	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ. Программный компонент СОВ. Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	4	
	Практическое занятие Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2	
Раздел 3. Защита информации в локальных сетях		16	
Тема 1. Основы построения защищенных сетей	Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	4	
Тема 2. Средства организации VPN	Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN.	5	
	Самостоятельная работа Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура,	5	

	модель нарушителя, достоинства и недостатки		
	Практическое занятие Развертывание VPN	2	
Раздел 4. Защита информации в сетях общего доступа		27	
Тема 1.Обеспечение безопасности межсетевого взаимодействия	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	10	
	Самостоятельная работа Уровень 3. Proxy-сервера прикладного уровня Однохостовые и мультихостовые firewall Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций Требования по сертификации межсетевых экранов Тематика практических занятий и лабораторных работ	10	
	Практическое занятие Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. Изучение различных способов закрытия "опасных" портов	7	
Раздел 5. Защита информации в базах данных		16	
Тема 1. Защита информации в базах данных	Основные типы угроз. Модель нарушителя Средства идентификации и аутентификации. Управление доступом Средства контроля целостности информации в базах данных Средства аудита и контроля безопасности.	8	
	Самостоятельная работа Критерии защищенности баз данных Применение криптографических средств защиты информации в базах данных	5	
	Практические занятия Изучение механизмов защиты СУБД MS	3	

	Access Изучение штатных средств защиты СУБД MSSQL Server		
Раздел 6. Мониторинг систем защиты		31	
Тема 1. Мониторинг систем защиты	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25 Классификация отслеживаемых событий. Особенности построения систем мониторинга Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования Классификация сетевых мониторов Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке	10	
	Практическое занятие Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов Проведение аудита ЛВС сетевым сканером	5	
Тема 2. Изучение мер защиты информации в информационных системах	Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты	4	
	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 3. Изучение современных программно-аппаратных комплексов.	**Практическое занятие** Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение	10	

	функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов Изучение типовых решений для построения VPN на примере VipNet или других аналогов Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов		
Курсовая работа		26	
Консультации		2	
Примерная тематика курсовых работ Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) Проблема защиты информации в облачных хранилищах данных и ЦОДах Защита сред виртуализации			
Примерная тематика самостоятельной работы при изучении МДК.02.01 Изучение новых технологий хранения информации Статистика и анализ крупных утечек информации за год Поиск информации о новых видах атак на информационную систему Обзор современных программных и программно-аппаратных средств защиты Сравнительный анализ современных программных и программно-аппаратных средств защиты			
Промежуточная аттестация по МДК.02.01		72	
Учебная практика по разделу 1 модуля 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			
Раздел 2 модуля. Применение криптографических средств защиты информации		240	
МДК.02.02. Криптографические средства защиты информации		186	
Раздел 1. Математические основы защиты информации		24	
Тема 1. Математические основы криптографии	Элементы теории множеств. Группы, кольца, поля. Делимость чисел. Признаки делимости. Простые и составные числа. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД. Отношения сравнимости. Свойства сравнений. Модулярная арифметика. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. Китайская теорема об остатках. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	12	
	Самостоятельная работа Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра. Арифметические операции над большими числами Эллиптические кривые и их приложения в криптографии	8	
	Практическое занятие	4	

	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений Решение задач с элементами теории чисел.		
Раздел 2. Классическая криптография		63	
Тема 1. Методы криптографического защиты информации	Классификация основных методов криптографической защиты. Методы симметричного шифрования. Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр. Методы перестановки.	10	
	Самостоятельная работа Табличная перестановка, маршрутная перестановка Гаммирование. Гаммирование с конечной и бесконечной гаммами.	4	
	Практическое занятие Применение классических шифров замены Применение классических шифров перестановки Применение метода гаммирования	14	
Тема 2. Криптоанализ	Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы.	7	
	Самостоятельная работа Принципы Киркхоффса Перспективные направления криптоанализа, квантовый криптоанализ.	4	
	Практическое занятие Криптоанализ шифра простой замены методом анализа частотности символов Криптоанализ классических шифров методом полного перебора ключей Криптоанализ шифра Вижинера	7	
Промежуточная аттестация по МДК.02.02			
Тема 3. Поточные шифры и генераторы псевдослучайных чисел	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	6	
	Самостоятельная работа Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	4	
	Практическое занятие Применение методов генерации ПСЧ	7	
Раздел 3. Современная криптография		147	

Тема 1. Кодирование информации. Компьютеризация шифрования.	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.	12	
	Самостоятельная работа Изучение современных программных и аппаратных криптографических средств	4	
	Практическое занятие Кодирование информации Программная реализация классических шифров Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	14	
Тема 2. Симметричные системы шифрования	Общие сведения. Структурная схема симметричных криптографических систем	5	
	Самостоятельная работа Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	4	
	Практическое занятие Изучение программной реализации современных симметричных шифров	7	
Тема 3. Асимметричные системы шифрования	Криптосистемы с открытым ключом. Необратимость систем.	5	
	Самостоятельная работа Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.	4	
	Практическое занятие Применение различных асимметричных алгоритмов. Изучение программной реализации асимметричного алгоритма RSA	8	
Тема 4. Аутентификация данных. Электронная подпись	Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	6	
	Самостоятельная работа Применение различных функций хеширования, анализ особенностей хешей	4	
	Практическое занятие Применение криптографических атак на	10	

	хеш-функции Изучение программно-аппаратных средств, реализующих основные функции ЭП		
Тема 5. Алгоритмы обмена ключей и протоколы аутентификации	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	8	
	Самостоятельная работа Применение протокола Диффи-Хеллмана для обмена ключами шифрования. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	4	
	Практическое занятие Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	5	
Тема 6. Криптозащита информации в сетях передачи данных	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP	8	
Тема 7. Защита информации в электронных платежных системах	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер.	10	
	Самостоятельная работа Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	4	
	Практическое занятие Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей	7	
Тема 8. Компьютерная стеганография	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав.	7	
	Самостоятельная работа Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	4	
	Практическое занятие	7	

	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ Реализация простейших стеганографических алгоритмов		
Примерная тематика самостоятельной работы при изучении МДК.02.02 История развития криптографии Программная реализация классических шифров Оптимизация методов частотного анализа моноалфавитных шифров. Программная реализация классических шифров Методы механизации шифрования Цифровое представление различных форм информации Анализ современных симметричных криптоалгоритмов Анализ современных асимметричных криптоалгоритмов Программная реализация современных криптоалгоритмов			
Консультации		2	
Промежуточная аттестация по МДК.02.02		72	
Производственная практика по ПМ.02 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.			
Экзамен по профессиональному модулю		6	
ВСЕГО		720	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета:

- автоматизированные рабочие места обучающихся;
- компьютеры, объединенные в локальную вычислительную сеть;
- проектор;
- экран;
- акустическая система;
- учебно-наглядные пособия:
- схемы;
- таблицы;
- учебные презентации.
- Раздаточный дидактический материал: учебные карточки с заданиями; дидактический материал для выполнения практических работ.

Технические средства обучения:

- компьютеры, объединенные в локальную вычислительную сеть;
- мультимедиа проектор;
- интерактивная доска.
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности в виде: ПАК Соболь (имеется в наличии) – 1шт.
- Учебно-методические материалы и образы виртуальных машин для развертывания учебных стендов по следующим темам: "Защита серверов и рабочих станций" (Основы применения системы защиты Secret Net Studio, Secret Net LSP и ПАК "Соболь") – от 16 до 32 академических часов; "Защита сетевого периметра" (Основы применения АПКШ "Континент" версий 3.9, 4 для организации сетевой защиты) – от 16 до 32 академических часов; "Организация доступа удаленных пользователей к веб-ресурсам защищаемой корпоративной сети по протоколу TLS" (Основы применения СКЗИ "Континент TLS" для организации удаленного доступа) – от 8 до 16 академических часов; "Защита средств виртуализации" (Основы применения vGate для защиты виртуальных инфраструктур) – 8–12 академических часов

Оснащение лаборатории Информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники по одному рабочему месту на обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»;
- Дистрибутивы программного комплекса Vipnet;
- Дистрибутивы программного комплекса InfoWatch TrafficMonitor
- Дистрибутивы Linux операционных систем;
- Дистрибутивы антивирусных программных комплексов;

- Академическая подписка Office 365 A1 для преподавателей и студентов;
- программное обеспечение: дистрибутивы операционных систем; правочная правовая система «Гарант»; ПО Oracle VirtualBox; антивирусная программа;
- Прикладное программное обеспечение, в том числе: Академическая подписка Office 365 A1 для преподавателей и студентов;
  Бесплатное ПО: LibreOffice - офисный пакет с открытым исходным кодом, являющийся ответвлением от проекта OpenOffice.org и претендующий на роль бесплатной альтернативы пакету офисных приложений Microsoft Office. В состав программы входят текстовый редактор Writer, табличный процессор Calc, мастер презентаций Impress, векторный графический редактор Draw, редактор формул Math и модуль управления базами данных Base; GIMP - свободно распространяемый растровый графический редактор, программа для создания и обработки растровой графики и частичной поддержкой работы с векторной графикой (Аналог Adobe Photoshop); Inkscape - Свободно распространяемый векторный графический редактор, удобен для создания как художественных, так и технических иллюстраций. (аналог Adobe Illustrator, Corel Draw и MicrosoftVisio)
- специализированное программное обеспечение: EclipseIDEforJavaEEDevelopers, .NETFrameworkJDK 8, MicrosoftSQLServerExpressEdition, MicrosoftVisioProfessional, MicrosoftVisualStudio Community, SQLServerManagementStudio, MicrosoftSQLServerJavaConnector, AndroidStudio, Cisco Packet Tracer (на правах сетевой академии Cisco), Oracle VirtualBox, Пакет All Products Pack IDE от JetBrains (Академическая лицензия).
- программные и программно-аппаратные средства обнаружения вторжений (Secret Net Studio);
- средства уничтожения остаточной информации в запоминающих устройствах: ПО низкоуровневого форматирования информации;
- Установочные комплекты Secret Net Studio, Secret Net LSP и vGate с набором учебных лицензий на 3 года бесплатно для развертывания в учебном классе;

- Выход в электронно-информационную образовательную среду колледжа (порядок доступа к элементам ЭИОС и отдельным информационным базам и системам): https://moodle.yakit.ru

3.2. Информационное обеспечение обучения

3.2.1 Основные печатные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/495525U

2. 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: Uhttps://urait.ru/bcode/497433U

3. 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: 8TUhttps://urait.ru/bcode/497433

4. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 383 с. — (Профессиональное образование). — ISBN 978-5-534-03051-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/489603U

5. 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: Uhttps://urait.ru/bcode/497433U

6. 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: Uhttps://urait.ru/bcode/498889U

7. Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — Москва : Издательство Юрайт, 2022. — 235 с. — (Профессиональное образование). — ISBN 978-5-534-05047-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/492496U

8. Тузовский, А. Ф. Проектирование и разработка web-приложений : учебное пособие для среднего профессионального образования / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2022. — 218 с. — (Профессиональное образование). — ISBN 978-5-534-10017-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/495109U

9. Черткова, Е. А. Программная инженерия. Визуальное моделирование программных систем : учебник для среднего профессионального образования / Е. А. Черткова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 147 с. — (Профессиональное образование). — ISBN 978-5-534-09823-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/493226U

3.2.2. Дополнительная литература

1. 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: Uhttps://urait.ru/bcode/498889U

2. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/494562U

3. Новожилов, О. П. Информатика в 2 ч. Часть 1 : учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 320 с. — (Профессиональное образование). — ISBN 978-5-534-06372-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/493964U8T

4. Новожилов, О. П. Информатика в 2 ч. Часть 2 : учебник для среднего профессионального образования / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 302 с. — (Профессиональное образование). — ISBN 978-5-534-06374-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/493965

5. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2022. — 258 с. — (Профессиональное образование). — ISBN 978-5-534-03173-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/491568U

6. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: 8TUhttps://urait.ru/bcode/495525U8T

7. Стасышин, В. М. Базы данных: технологии доступа : учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/494562U

8. Тузовский, А. Ф. Проектирование и разработка web-приложений : учебное пособие для среднего профессионального образования / А. Ф. Тузовский. — Москва : Издательство Юрайт, 2022. — 218 с. — (Профессиональное образование). — ISBN 978-5-534-10017-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/495109U

9. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк,

Н. Б. Ничепорук ; под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2022. — 258 с. — (Профессиональное образование). — ISBN 978-5-534-03173-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/491568U

10. Гаврилов, М. В. Информатика и информационные технологии : учебник для среднего профессионального образования / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 383 с. — (Профессиональное образование). — ISBN 978-5-534-03051-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/489603U

11. Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — Москва : Издательство Юрайт, 2022. — 235 с. — (Профессиональное образование). — ISBN 978-5-534-05047-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: Uhttps://urait.ru/bcode/492496U

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты обучения **(освоенные умения, усвоенные знания)**	**Формы и методы контроля и оценки результатов обучения**
Умения:	
-устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	Практические занятия, домашняя работа, тестирование
-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 а так.	
Знания:	
особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	Домашняя работа, тестирование
-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.	
особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;	