приложение 1.2

к ОПОП по специальности
10.02.05 Обеспечение информационной
безопасности автоматизированных систем

АДАПТИРОВАННАЯ РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

для обучающихся с расстройством аутистического спектра

СОДЕРЖАНИЕ

ОБЩАЯ ХАРАКТЕРИСТИКА АДАПТИРОВАННОЙ РАБОЧЕЙ ПРОГРАММЫ 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:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	**Защита информации в автоматизированных системах программными и программно-аппаратными средствами**
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.1.2. Общие компетенции

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

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

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

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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. Пользоваться профессиональной документацией на государственном и иностранном языках.

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.
уметь	− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; − диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; − применять программные и программно-аппаратные средства для защиты информации в базах данных; − проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; − применять математический аппарат для выполнения криптографических преобразований; − использовать типовые программные криптографические средства, в том числе электронную подпись; − применять средства гарантированного уничтожения информации; − устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	− особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных

	системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 504 час, из них

на освоение МДК – 342 часов,

производственная практика – 144 час.,

экзамен по профессиональному модулю – 18 ч.

2. СТРУКТУРА И СОДЕРЖАНИЕ 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	
			всего, часов	в том числе			учебная практика, часов	производственная практика, часов
				лабораторных и практических занятий	курсовая работа (проект), часов	Сам.работа/консультации		
ПК 2.1 – ПК 2.6 ОК 1-ОК 9	**Раздел 1 модуля.** Применение программных и программно-аппаратных средств защиты информации	**256**	**184**	54	30	27/27	-	72
ПК 2.4 ОК 1-ОК 9	**Раздел 2 модуля.** Применение криптографических средств защиты информации	**230**	**158**	60	–	13/13	-	72
	Промежуточная аттестация	**-**	**-**	–	–	-	–	–
	Экзамен по профессиональному модулю	**18**	**-**	–	–	-	–	–
	Всего:	**504**	**342**	104	30	40/40	-	**144**

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
1	2	3
Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации		
МДК.02.01. Программные и программно-аппаратные средства защиты информации		
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации		
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации	**Содержание**	
	ТЗ.1 Предмет и задачи программно-аппаратной защиты информации	2
	ТЗ.2 Основные понятия программно-аппаратной защиты информации	2
	ТЗ.3 Классификация методов и средств программно-аппаратной защиты информации	2
Тема 1.2. Стандарты безопасности	**Содержание**	
	ТЗ.4 Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)	2
	ТЗ.5 Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.1 Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. П З . 2 Работа с содержанием нормативных правовых актов.	2 2 2
	ПЗ.3 Обзор стандартов. Работа с содержанием стандартов	
Тема 1.3. Защищенная	**Содержание**	

автоматизированная система	ТЗ.6 Автоматизация процесса обработки информации	2
	Понятие автоматизированной системы.	
	Особенности автоматизированных систем в защищенном исполнении.	
	Основные виды АС в защищенном исполнении.	
	ТЗ.7 Методы создания безопасных систем	2
	Методология проектирования гарантированно защищенных КС	
	Дискреционные модели	
	Мандатные модели	
	Тематика практических занятий и лабораторных работ	
	ПЗ.4 Учет, обработка, хранение и передача информации в АИС	2
	Ограничение доступа на вход в систему.	2
	Идентификация и аутентификация пользователей	2
	ПЗ.5 азграничение доступа.	
	Регистрация событий (аудит).	
	Контроль целостности данных	
	ПЗ.6 Уничтожение остаточной информации.	
	Управление политикой безопасности. Шаблоны безопасности	
	СР.1 Криптографическая защита. Обзор программ шифрования данных	2
	СР.2 Управление политикой безопасности. Шаблоны безопасности	2
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	
	ТЗ.8 Источники дестабилизирующего воздействия на объекты защиты	2
	ТЗ.9 Способы воздействия на информацию	2
	СР.3 Причины и условия дестабилизирующего воздействия на информацию	1
	Тематика практических занятий и лабораторных работ	
	ПЗ.7,8 Распределение каналов в соответствии с источниками воздействия на информацию	2 2
Тема 1.5. Принципы программно-аппаратной защиты информации от	**Содержание**	
	ТЗ.10 Понятие несанкционированного доступа к информации	2
	К.1 Основные подходы к защите информации от НСД	2

несанкционированного доступа	ТЗ.11 Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам	2
	ТЗ.12 Доступ к данным со стороны процесса	
	К.2 Особенности защиты данных от изменения. Шифрование.	2 2
	Тематика практических занятий и лабораторных работ	
	ПЗ.9 Организация доступа к файлам	2
	ПЗ.10 Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД	2
	К.3	1
Промежуточная аттестация в форме контрольной работы		-
	Итого за семестр	54
Раздел 2. Защита автономных автоматизированных систем		
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**	
	ТЗ.1 Работа автономной АС в защищенном режиме	2
	Алгоритм загрузки ОС. Штатные средства замыкания среды	2
	ТЗ.2 Расширение BIOS как средство замыкания программной среды	2
	Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка)	
	ТЗ.3 Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	
Тема 2.2.Защита программ от изучения	**Содержание**	
	ТЗ.4 Изучение и обратное проектирование ПО	2
	Способы изучения ПО: статическое и динамическое изучение	2
	ТЗ.5 Задачи защиты от изучения и способы их решения	2
	Защита от отладки.	
	ТЗ.6 Защита от дизассемблирования	
	Защита от трассировки по прерываниям.	
Тема 2.3. Вредоносное программное обеспечение	**Содержание**	
	ТЗ.7 Вредоносное программное обеспечение как особый вид разрушающих воздействий	2

	Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения	2
	ТЗ.8 Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие	

	информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch.	
	Бот-неты. Принцип функционирования. Методы обнаружения	
	Классификация антивирусных средств. Сигнатурный и эвристический анализ	
	Защита от вирусов в "ручном режиме"	
	Основные концепции построения систем антивирусной защиты на предприятии	
	Тематика практических занятий и лабораторных работ	
	ПЗ.1 Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	
	ТЗ.9 Несанкционированное копирование программ как тип НСД	2
	Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования.	2
	ТЗ.10 Привязка ПО к аппаратному окружению и носителям.	
	Защитные механизмы в современном программном обеспечении на примере MS Office	
	Тематика практических занятий и лабораторных работ	
	ПЗ.2 Защита информации от несанкционированного копирования с использованием специализированных программных средств	2
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint)	
Тема 2.5. Защита информации на машинных носителях	**Содержание**	
	ТЗ.11 Проблема защиты отчуждаемых компонентов ПЭВМ.	2
	Методы защиты информации на отчуждаемых носителях. Шифрование.	2
	К.1 Средства восстановления остаточной информации. Создание посекторных образов НЖМД.	2
	К.2 Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов	
	Безвозвратное удаление данных. Принципы и алгоритмы.	
	Тематика практических занятий и лабораторных работ	

	ПЗ.3 Применение средства восстановления остаточной информации на примере Foremost или аналога	2
	ПЗ.4 Применение специализированного программно средства для восстановления удаленных файлов	2
	ПЗ.5 Применение программ для безвозвратного удаления данных	2
	ПЗ.6 Применение программ для шифрования данных на съемных носителях	2
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	
	К.3 Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ	2 2
	К.4 Устройства Touch Memory	
Тема 2.7. Системы обнаружения атак и вторжений	**Содержание**	
	К.5 СОВ и СОА, отличия в функциях. Основные архитектуры СОВ	2
	Использование сетевых снифферов в качестве СОВ	2
	Аппаратный компонент СОВ	
	Программный компонент СОВ	
	К.6 Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	
	Тематика практических занятий и лабораторных работ	
	ПЗ.7 Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	2
Раздел 3. Защита информации в локальных сетях		
Тема 3.1. Основы построения защищенных сетей	**Содержание**	
	К.7 Сети, работающие по технологии коммутации пакетов	2
	Стек протоколов TCP/IP. Особенности маршрутизации.	2
	Штатные средства защиты информации стека протоколов TCP/IP.	
	К.8 Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	
Тема 3.2. Средства организации VPN	**Содержание**	
	К.9 Виртуальная частная сеть. Функции, назначение, принцип построения	2
	Криптографические и некриптографические средства организации VPN	2
	Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр.	

	К.10 Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	
	Тематика практических занятий и лабораторных работ	
	ПЗ.8 Развертывание VPN	2
Раздел 4. Защита информации в сетях общего доступа		
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия	**Содержание**	
	К.11 Методы защиты информации при работе в сетях общего доступа.	2
	Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности	2
	Основные типы firewall. Симметричные и несимметричные firewall.	2
	СР.1 Уровень 1. Пакетные фильтры	2
	Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне.	
	Уровень 3. Proxy-сервера прикладного уровня	
	СР.2 Однохостовые и мультихостовые firewall.	
	Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций	
	СР.3 Требования по сертификации межсетевых экранов	
	Тематика практических занятий и лабораторных работ	
	ПЗ.9 Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	2
	ПЗ.10 Изучение различных способов закрытия "опасных" портов	2
Раздел 5. Защита информации в базах данных		
Тема 5.1. Защита информации в базах данных	**Содержание**	
	СР.4 Основные типы угроз. Модель нарушителя	2
	Средства идентификации и аутентификации. Управление доступом	2
	СР.5 Средства контроля целостности информации в базах данных	2
	Средства аудита и контроля безопасности. Критерии защищенности баз данных	
	СР.6 Применение криптографических средств защиты информации в базах данных	
	Тематика практических занятий и лабораторных работ	
	ПЗ.11 Изучение механизмов защиты СУБД MS Access	2

	ПЗ.12 Изучение штатных средств защиты СУБД MSSQL Server	2
Раздел 6. Мониторинг систем защиты		
Тема 6.1. Мониторинг систем защиты	**Содержание**	
	СР.7 Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации	2 2 2
	Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25	
	СР.8 Классификация отслеживаемых событий. Особенности построения систем мониторинга	
	Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования.	
	СР.9 Классификация сетевых мониторов	
	Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	
	Тематика практических занятий и лабораторных работ	
	ПЗ.13 Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов	2
	Проведение аудита ЛВС сетевым сканером	
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	
	СР.10 Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.14 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.	**Тематика практических занятий и лабораторных работ**	
	ПЗ.15 Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов	2 2 2 2
	ПЗ.16 Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других	

	аналогов	
	ПЗ.17 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	
	СР.11 Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов	
Промежуточная аттестация в форме защиты курсовой работы		**30**
Примерная тематика курсовых 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		

Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.		
Итого за семестр		**130**
Производственная практика по разделу 1 **ПП.02.01**		**72**
ВСЕГО ПО РАЗДЕЛУ 1		**202**
Раздел 2 модуля. Применение криптографических средств защиты информации		
МДК.02.02. Криптографические средства защиты информации		
Введение	**Содержание**	
	ТЗ.1 Предмет и задачи криптографии. История криптографии. Основные термины	2
Раздел 1. Математические основы защиты информации		
Тема 1.1. Математические основы криптографии	**Содержание**	
	ТЗ.2 Элементы теории множеств. Группы, кольца, поля.	2
	ТЗ.3 Делимость чисел. Признаки делимости. Простые и составные числа.	2
	ТЗ.4 Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2 2
	ТЗ.5 Отношения сравнимости. Свойства сравнений. Модулярная арифметика.	2
	ТЗ.6 Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм	

	быстрого возведения в степень по модулю.	2
	ТЗ.7 Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида.	2
	ТЗ.8 Китайская теорема об остатках.	2
	ТЗ.9 Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.	2 2 2
	ТЗ.10 Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2
	ТЗ.11 Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.	2
	ТЗ.12 Арифметические операции над большими числами.	2
	К.1 Эллиптические кривые и их приложения в криптографии.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.1 Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	2 2
	ПЗ.2 Проверка чисел на простоту	2
	ПЗ.3 Решение задач с элементами теории чисел.	
Раздел 2. Классическая криптография		
Тема 2.1. Методы криптографического защиты информации	**Содержание**	
	К.2 Классификация основных методов криптографической защиты. Методы симметричного шифрования	2 2
	СР.1 Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2
	СР.2 Методы перестановки. Табличная перестановка, маршрутная перестановка	
	Гаммирование. Гаммирование с конечной и бесконечной гаммами	
	Тематика практических занятий и лабораторных работ	
	ПЗ.4 Применение классических шифров замены	2
	ПЗ.5 Применение классических шифров перестановки	2
	ПЗ.6 Применение метода гаммирования	2
Тема 2.2. Криптоанализ	**Содержание**	
	К.3 Основные методы криптоанализа. Криптографические атаки.	1
	СР.3 Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса	1
	Перспективные направления криптоанализа, квантовый криптоанализ.	
	Тематика практических занятий и лабораторных работ	

	ПЗ.7 Криптоанализ шифра простой замены методом анализа частотности символов	2
	ПЗ.8,9 Криптоанализ классических шифров методом полного перебора ключей	2
	ПЗ.10 Криптоанализ шифра Вижинера	2
		2
Промежуточная аттестация в форме контрольной работы		-
	Итого за семестр	**54**
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	
	ТЗ.1 Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2
	ТЗ.2 Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.1 Применение методов генерации ПСЧ	2
Раздел 3. Современная криптография		
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	
	ТЗ.3 Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII	2
	ТЗ.4 Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств.	2
	ТЗ.5 Изучение современных программных и аппаратных криптографических средств	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.2 Кодирование информации	2
	ПЗ.3 Программная реализация классических шифров	2
	ПЗ.4,5 Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2
		2
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	
	ТЗ.6 Общие сведения. Структурная схема симметричных криптографических систем	2
	ТЗ.7 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	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.6,7 Изучение программной реализации современных симметричных шифров	2
		2

Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	
	ТЗ.8 Криптосистемы с открытым ключом. СР.1 Необратимость систем. СР.2 Структурная схема шифрования с открытым ключом.	2 2 2 2
	ТЗ.9 Элементы теории чисел в криптографии с открытым ключом.	
	Тематика практических занятий и лабораторных работ	
	ПЗ.8 Применение различных асимметричных алгоритмов.	2
	ПЗ.9 Изучение программной реализации асимметричного алгоритма RSA	2
Тема 3.4. Аутентификация данных. Электронная подпись	**Содержание учебного материала**	
	ТЗ.10 Аутентификация данных. Общие понятия. ЭП. МАС. СР.3 Однонаправленные хеш-функции. ТЗ.11 Алгоритмы цифровой подписи	2 2 2
	Тематика практических занятий и лабораторных работ	
	ПЗ.10 Применение различных функций хеширования, анализ особенностей хешей	2
	ПЗ.11 Применение криптографических атак на хеш-функции.	2
	ПЗ.12,13 Изучение программно-аппаратных средств, реализующих основные функции ЭП	2 2
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	
	ТЗ.12 Алгоритмы распределения ключей с применением симметричных и асимметричных схем ТЗ.13 Протоколы аутентификации. К.1 Взаимная аутентификация. СР.4 Односторонняя аутентификация	2 2 2 2
	Тематика практических занятий и лабораторных работ	
	ПЗ.14 Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2
	ПЗ.15,16 Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2 2
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	
	ТЗ.14 Абонентское шифрование. Пакетное шифрование. ТЗ.15 Защита центра генерации ключей.	2 2

	ТЗ.16 Криптомаршрутизатор. Пакетный фильтр	2
	ТЗ.17 Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2
Тема 3.7. Защита	**Содержание учебного материала**	

информации в электронных платежных системах	ТЗ.18 Принципы функционирования электронных платежных систем. ТЗ.19 Электронные пластиковые карты. ТЗ.20 Персональный идентификационный номер	2 2 2
	ТЗ.21 Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.17 Применение аутентификации по одноразовым паролям. ПЗ.18 Реализация алгоритмов создания одноразовых паролей	2 2
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	
	ТЗ.22 Скрытая передача информации в компьютерных системах. ТЗ.23 Проблема аутентификации мультимедийной информации. ТЗ.24 Защита авторских прав.	2 2 2 2
	К.2 Методы компьютерной стеганографии. К.3 Цифровые водяные знаки. К.4 Алгоритмы встраивания ЦВЗ	2 2 2
	Тематика практических занятий и лабораторных работ	
	ПЗ.19 Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	2
	ПЗ.20 Реализация простейших стеганографических алгоритмов	2
Промежуточная аттестация в форме дифференцированного зачета		**-**
	Итого за семестр	**104**
Производственная практика по разделу 2 ПП.02.02		**72**
	ВСЕГО ПО РАЗДЕЛУ 2	**176**

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	18
Всего:	**504**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Программных и программно-аппаратных средств обеспечения информационной безопасности», оснащенная в соответствии с ОПОП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики, в соответствии с ОПОП по данной специальности.

3.1.1 Требования к материально-техническому обеспечению обучающихся с РАС

В учебных аудиториях (по возможности) стараться избегать использования ламп дневного света с дросселями, т.к. они мерцают и издают гул. Преимущественное использование светодиодов или ламп дневного света с качественным электронным балластом.

В аудиториях не должно быть гула или стробоскопического эффекта. Обеспечение хорошей акустики: не должно быть эха, посторонних шумов и т.п.

3.2 Реализация адаптированной программы профессионального модуля предполагает обязательную учебную и производственную практики.

Требования к оснащению баз практик в соответствии с п. 6.3.7 АОП СПО по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Требования к организации практической подготовки обучающихся с инвалидностью и/или ограниченными возможностями здоровья (РАС)

Для обучающихся с РАС проведение практической подготовки устанавливается образовательной организацией с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья. При определении мест прохождения учебной и производственных практик, обучающихся с РАС образовательная организация должна учитывать рекомендации, данные по результатам медико-социальной экспертизы, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда. (например, при непреодолимых препятствиях: непереносимости запахов в лаборатории, шумов в цехах и т.п.)

3.3 Информационное обеспечение реализации адаптированной программы

3.3.1 Для реализации адаптированной программы библиотечный фонд колледжа имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе.

При формировании библиотечного фонда выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

Обучающиеся инвалиды и лица с ограниченными возможностями здоровья обеспечены печатными и (или) электронными учебными изданиями, адаптированными при необходимости для обучения указанных обучающихся.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется настоящей адаптированной рабочей программой и подлежит обновлению (при необходимости).

3.3.2. Учебно-методическое обеспечение реализации адаптированной программы обучающихся с РАС

Предоставление презентаций, конспектов, видеозаписей занятий и т.п. Структурировано оформленные фонды оценочных средств. Дополнительные подробные инструкции и пояснения для выполнения задания.

3.3.3 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, 2024. — 161 с. — (Профессиональное

образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340.

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580668.

3. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561717.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
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 профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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 профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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 по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения

		ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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 профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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, экзамен по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, экзамен по профессиональному модулю, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике

компьютерных атак.		
ОК 01.Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на практических занятиях, при выполнении работ по производственной практике Экзамен по профессиональному модулю
ОП 02.Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями производственной практики; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;	- соблюдение норм поведения во время учебных занятий и прохождения производственной практике	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении производственной практике; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении производственной практике;	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

Для осуществления процедур текущего контроля успеваемости, промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для обучающихся инвалидов и лиц с ограниченными возможностями здоровья, позволяющие оценить достижение ими результатов обучения и уровень сформированности всех компетенций, предусмотренных адаптированной образовательной программой.

Форма проведения текущей аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа при прохождении аттестации.