Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

квалификация
техник по защите информации

Белгород 2020 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**, примерной основной образовательной программы (разработчик ПООП: **Федеральное учебно-методическое объединение в системе среднего профессионального образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность», 2017 год).**

Рассмотрено цикловой комиссией Протокол заседания № 1 от «31» августа 2020г. Председатель цикловой комиссии _____/Чобану Л.А./	Согласовано Зам.директора по УМР _____/Бакалова Е.Е. «31» августа 2020 г.	Утверждаю Зам.директора по УР _____ /Выручаева Н.В. «31» августа 2020 г.
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2021 г. Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2022 г Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2023 г Председатель цикловой комиссии _____/_____		

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:
преподаватель ОГАПОУ «Белгородский индустриальный колледж» Внукова Н.В.
Экспертиза:
(*внутренний рецензент*) ОГАПОУ «Белгородский индустриальный колледж», преподаватель ОГАПОУ «Белгородский индустриальный колледж» Солдатенко М.Н.
(*внешний рецензент*) Генеральный директор ООО «Фортуна» Мочалов В.И.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности (специальностям) СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности ВД 1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты и соответствующие ему общие компетенции, и профессиональные компетенции:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

1.2.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	**Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты**
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3.	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

1.2.3. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	– определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации; – установки, настройки специализированного оборудования криптографической защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; шифрования информации;
уметь	– выявлять и оценивать угрозы безопасности

	информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
знать	– типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; – основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; – основные понятия криптографии и типовые криптографические методы защиты информации.

1.4. Рекомендуемое количество часов на освоение программы профессионального модуля:

Всего часов –716, в том числе:

на освоение МДК, в том числе промежуточную аттестацию –422 часа;

на практики, в том числе

учебную–72 часа;

производственную –216 часов;

консультации – 8 часов;

самостоятельную работу – 14 часов;

промежуточная аттестация – 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

2.1. Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Занятия во взаимодействии с преподавателем, час						Самостоятельная работа обучающегося	Консультации
			Обучение по МДК, в час.				Практики			
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Промежуточная аттестация	Учебная	Производственная		
1	2	3	4	5	6	7	8	9	10	11
ОК1-4, ОК9,10 ПК 2.1-2.3	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**254**	**244**	66	20	-			**8**	**2**
ОК1-4, ОК9,10 ПК 2.1-2.3	Раздел 2. Криптографическая защита информации	**168**	**150**	44	10	**6**			**6**	**6**
	Учебная практика	**72**					**72**			
ОК1-4, ОК9,10 ПК 2.1-2.3	**Производственная практика (по профилю специальности)**	**216**						**216**		
Экзамен по модулю		**6**				**6**				
Всего:		**716**	**394**	110	30	**12**	**72**	**216**	**14**	**8**

2.2. Тематический план и содержание обучения по профессиональному модулю ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, курсовая работ (проект) *(если предусмотрены)*		Объем часов
1	**2**		**3**
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**254**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**254**
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**		**64**
	1.	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. Windows 7. Windows8. Linux. QNX и другие операционные системы.	
	2.	Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя.Методы аутентификации	
	3.	Пароли. PIN-коды. Методы надежного составления паролей.	
	4.	Строгая аутентификация.	
	5.	Односторонняя аутентификация. Двухсторонняя аутентификация	
	6.	Аппаратно-программные средства идентификации и аутентификации.	
	7.	Токены. Смарт-карты. Виртуальные ключи.	
	8.	Программно-аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ.	
	9.	АПМДЗ Криптон –Замок системный администратор. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ.	
	10.	Ограничения действий пользователя. Идентификация. Журнал регистрации событий.	

		Настройки целостности среды АПМДЗ	
	11.	Сектор НЖМД. Область памяти. Файл, папка, каталог.	
	Лабораторные работы		16
	1.	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя	
	2.	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	
	3.	Настройка изолированной среды	
	4.	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	
	5.	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	
	6.	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	
	7.	Восстановление информации типовыми средствами Программы восстановление информации	
Тема 1.2. Технологии разграничения доступа	**Содержание**		**52**
	1.	Архитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Server2016. Возможности администратора.	
	2.	Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли.	
	3.	Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы.	
	4.	Изолированная программная среда. Способы организации. Методы применения.	
	5.	ActiveDirectory. Комплексная система организации управления доступом. Инсталляция. Настройка.	
	6.	Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита.	
	7.	Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции.	

		Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов.	
	8.	Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня.	
	9.	Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ.	
	10.	Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	
	Лабораторные работы		10
	1.	Программы надежного удаления информации	
	2.	Архивирование информации	
	3.	Программные средства резервного копирования. Настройка RAID-массивов	
	4.	Инсайдерская информация. Программы сбора информации о ПК	
	5.	Настройка межсетевого экрана	
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание**		**72**
	1.	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях.	
	2.	Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование.	
	3.	VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Туннелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация.	
	4.	Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.	
	5.	Защита на сетевом уровне.	

		Архитектура средств безопасности IPSec, AH, ESP.	
	6.	Защита на прикладном уровне.	
	7.	Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.	
	8.	Web-доступ. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos.	
	Лабораторные работы		36
	1.	Основные действия с виртуальной машиной	
	2.	Работа с контрольными точками	
	3.	Использование внешних устройств	
	4.	Работа с локальным хранилищем сертификатов в ОС WINDOWS	
	5.	Установка и настройка ПО eTokenPKIClient	
	6.	Настройка ПО eTokenPKIClient с помощью групповых политик	
	7.	Развертывание TMS в среде Active Directory	
	8.	Настройка TMS всреде Active Directory	
	9.	Настройкаполитик TMS	
	10.	Настройка использования виртуального токена	
	11.	Использование токена на рабочем месте администратора	
	12.	Установка и настройка СКЗИ «КриптоПроCSP»	
	13.	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами КриптоПроCSP	
	14.	Применение SecretDisk4	
	15.	Применение SecretDisk Server NG	
	16.	Изучение основных возможностей ПО VipNetClient	
	17.	Изучение настроекПОVipNetClient	
	18.	Изучение возможностей ПО Деловая почта	
Тема 1.4. Технологии обнаружения вторжений	**Содержание**		**22**
	1.	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности.	
	2.	Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	
	3.	Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак.	

		Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях.Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак.	
	4.	Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	
	Лабораторные работы		4
	1.	Изучение средств обнаружения атак	
	2.	Изучение антивирусных продуктов	
Тема 1.5. Методы управления средствами защиты	**Содержание**		**14**
	1.	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты.	
	2.	Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности.	
	3.	Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	
Самостоятельная работа при изучении МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты Работа с конспектами, учебной и специальной литературой (по параграфам, главам учебных пособий, указанным преподавателем). Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, оформление лабораторных работ и подготовка их к защите. Работа над курсовым проектом, подготовка к его защите. **Примерная тематика домашних заданий** 1. Проблемы обеспечения безопасности операционных системWindowsXP. Windows 7. Windows8. Linux. QNX. 2.Технологии аутентификации. 3.Аутентификация, авторизация и администрирование действий пользователя. 4.Пароли. PIN-коды. Методы надежного составления паролей. 5.Токены. Смарт-карты. Виртуальные ключи. 6.Программно-аппаратные модули доверенной загрузки.			**8**

7.АПМДЗ Криптон –Замок системный администратор. 8.Изучение настроек системного администратора АПМДЗ. 9.Сектор НЖМД. Область памяти. Файл, папка, каталог. 10.Разграничение доступа к объектам операционной системы. 11.Комплексная система организации управления доступом. Инсталляция. Настройка. 12.Аудит безопасности операционной системы. 13.Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 14.Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 15.Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. 16.Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. 17.Концепция построения виртуальных защищенных сетей. 18.Виртуальные защищенные сети. Туннелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов. 19.Защита на канальном уровне. ПротоколыPPTP, L2F, L2TP. 20.Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. 21.Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. 22.Защита на прикладном уровне. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos. Функционирование системы управления средствами защиты. 24.Аудит безопасности информационной системы.	
Консультации	**2**
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту)	**20**
Примерная тематика курсовых работ (проектов) 1. Модель угроз НСД на предприятии. 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии. 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии. 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии. 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии. 6. Построение модели нарушителя по требованиям ФСБ на предприятии. 7. Модель угроз безопасности ИС персональных данных на предприятии. 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с	

применением специализированных инструментов и методов (индивидуальное задание). 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание). 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание). 12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание). 13. Проблема защиты информации в облачных хранилищах данных и ЦОДах. 14. Защита сред виртуализации. 15. Файловая система EXT4FS с использованием WinHex. 16. СЗИ от НСД. 17. Система обнаружения вторжений SNORT. 18. Сканер уязвимостей Nessus. 19. Использование MetasploitFramework как инструмента пентеста. 20. Криминалистические исследования Windows. 21. Криминалистические исследования Android. 22. Применение утилит Elcomsoftware для восстановления парольной информации. 23. Сетевые атаки на компьютерные системы. Применение снифферов. 24. Сетевые атаки на компьютерные системы. Использование утилит удалённогоадминистрирования. 25. Система защиты информации КриптоПро. 26. Межсетевой экран iptables в Linux. 27. Технология BYOD. Тенденции, перспективы, проблемы, безопасность. 28. Защитные механизмы ОС Windows 10. 29. Защитные механизмы ОС Android. 30. Защитные механизмы MAC OS X. 31. Защитные механизмы IOS. 32. Инфраструктура и безопасность MicrosoftSystemCenter. 33. Механизмы работы и структура современных антивирусных средств. 34. Инструментарий KaliLinux. Назначение, возможности. 35. Механизмы защиты веб – браузеров (Opera, Firefox, Chrome, IE, Safari, Edge).		
Раздел 2. Криптографическая защита информации		**168**
МДК 02.02. Криптографическая защита информации		**168**
Тема 2.1. Основы криптографических методов защиты	**Содержание**	**44**
	1. Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые криптографическими	

информации		методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности.	
	2.	Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие.	
	3.	Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение.	
	4.	Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования.	
	5.	Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов.	
	6.	Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста.	
	7.	Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	
	Лабораторные работы		16
	1.	Стеганографические методы скрытия информации	
	2.	Бинарная арифметика. Модульная арифметика	
	3.	Применение методов шифрования перестановкой	
	4.	Применение методов шифрования заменой	
	5.	Применение методов шифрования многоалфавитной замены	
	6.	Криптоанализ методов перестановки	
	7.	Криптоанализ методов замены	
	8.	Компьютерное шифрование	
Тема 2.2. Современные стандарты шифрования	**Содержание**		**32**
	1.	Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES.	

	2.	Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015.	
	3.	Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos.	
	4.	Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля.	
	5.	Криптосистемы на основе метода эллиптических кривых. ЭЦП.	
	6.	Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	
	Лабораторные работы		4
	1.	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	
	2.	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**		**64**
	1.	Целостность сообщения. Случайная модель Orac1e. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции.	
	2.	Электронная цифровая подпись. Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012.	
	3.	Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены.	
	4.	Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI.	
	5.	Обеспечение безопасности сети с применением криптографических протоколов на	

		прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/M1ME.	
	6.	Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec.	
	7.	Организация VPN-сети Защита информации в сетях, организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16.	
	8.	Защита информации в сетях сотовой связи. А3. А8.А5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи.	
	9.	Криптовалюты. Биткоин. Блокчейн-системы Ethereum.	
	10.	Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.	
	Лабораторные работы		24
	1.	Разработка хэш-функции	
	2.	Разработка схемы простого пароля	
	3.	Разработка схемы динамического пароля	
	4.	Сертификаты открытого ключа	
	5.	Настройка и администрирование токена	
	6.	Настройка сервисов Рутокен-PinPad	
	7.	Настройка сервисов Рутокен-ЭЦП	
	8.	Настройка сервисов Рутокен–Bluetooth	
	9.	Настройка сервисов Рутокен–S	
	10.	Разработка алгоритма PGP	
	11.	Изучение протоколов SSL, TLS, IPSec	
	12.	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	
Самостоятельная работа при изучении раздела МДК 02.02. Криптографическая защита информации Работа с конспектами, учебной и специальной литературой (по параграфам, главам учебных пособий, указанным преподавателем). Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, оформление лабораторных работ и подготовка их к защите. Работа над курсовым проектом, подготовка к его защите.			**6**

Примерная тематика домашних заданий 1. Изучение новых технологий хранения информации. 2. Статистика и анализ крупных утечек информации за год. 3. Поиск информации о новых видах атак на информационную систему. 4. Обзор современных программных и программно-аппаратных средств защиты. 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты. 6. Криптографические методы. 7. Шифрование. Кодирование. Стеганография. Сжатие. 8. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. 9.Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов. 10. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 11. Компьютерное шифрование. 12. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 13. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. 14. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.	
Консультации	**6**
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту)	**10**
Примерная тематика курсовых работ (проектов) 1. Преобразование информации для сокрытия ее содержания. 2. Блочное и поточное шифрование. 3. Функционирование криптосистем. 4. Криптоанализ шифров перестановок. 5. Одноалфавитные и многоалфавитные замены. 6. Стандартные алгоритмы криптографической защиты сообщений. 7. Криптосистемы RSA. 8. Криптографические хэш-функции. 9. Классификация криптографических протоколов. 10. Понятие электронной цифровой подписи. 11. Протоколы распределения ключей ЭЦП.	
Экзамен	**6**
Учебная практика **Виды работ**	**72**

Выбор, подключение, настройка межсетевого экрана. Администрирование межсетевого экрана. Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования. Ознакомление, подключение, настройка системы антивирусной защиты. Администрирование системы антивирусной защиты. Составление алгоритма хеш-функции Составление алгоритма шифра Подключение, установка драйверов, настройка программных средств шифрования (Криптон или др.). Администрирование программных средств шифрования. Подключение, установка драйверов, настройка аппаратных средств шифрования. Администрирование аппаратных средств шифрования.	
Производственная практика (по профилю специальности) **Виды работ** Участие в организации работ по защите персональных компьютеров на предприятии. Участие в организации работ по защите локальных сетей на предприятии. Участие в организации работ по защите работ в глобальной сети интернет на предприятии. Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей. Подключение, установка драйверов, настройка программных средств абонентского шифрования. Администрирование внедренных средств. Настройка средств электронной подписи. Администрирование средств электронной подписи. Администрирование средств PKI.	**216**
Экзамен по модулю	**6**
Всего:	**716**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Программных и программно-аппаратных средств защиты информации».

Оборудование:

– рабочие места обучающихся, оборудованные персональными компьютерами;

– рабочее место преподавателя;

– аппаратные средства аутентификации пользователя;

– программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации;

– средства защиты информации от НСД, блокирования доступа и нарушения целостности.

Программное обеспечение:

– программные средства криптографической защиты информации;

– программные средства выявления уязвимостей и оценки защищенности ИТКС, анализа сетевого трафика;

– системы разграничения доступа;

– межсетевые экраны;

– средство криптографической защиты информации, реализующее функции удостоверяющего центра и создания виртуальных сетей;

– антивирусные программные комплексы.

Технические средства обучения:

– комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

Требования к оснащению баз практик

Реализация образовательной программы предполагает обязательную учебную и производственную практику.

Учебная практика реализуется в мастерских профессиональной образовательной организации и требует наличия оборудования, инструментов, расходных материалов, обеспечивающих выполнение всех видов работ, определенных содержанием программ профессиональных модулей в соответствии с выбранной траекторией, в том числе оборудования и инструментов, используемых при проведении чемпионатов WorldSkills и указанных в инфраструктурных листах конкурсной документации WorldSkills по компетенции «Анализ защищенности информационных систем от внешних угроз» (или ее аналогов).

Оборудование предприятий и технологическое оснащение рабочих мест производственной практики должно соответствовать содержанию деятельности и

давать возможность обучающемуся овладеть профессиональными компетенциями по всем осваиваемым видам деятельности, предусмотренным программой с использованием современных технологий, материалов и оборудования.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Бубнов, А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. - 3-е изд., стер. - М.: Академия, 2017. - 256 с. - (Профессиональное образование. Информационная безопасность).

2. Защита информационных технологий. Справочник: справочник / Ю.И. Коваленко. - М.: Русайнс, 2016. - 321 с. - http://www.book.ru/book/ 921524

3. Информационная безопасность.: учебник / Мельников В.П. под ред., Куприянов А.И. — Москва: КноРус, 2019. — 267 с. — (СПО).

4. Информационная безопасность: учебник / Мельников В.П. под ред., Куприянов А.И. — Москва: КноРус, 2019. — 267 с. — (СПО). — URL: https://book.ru/book/932059 (дата обращения: 01.11.2019). — Текст: электронный.

5. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи [Текст]: учебник для использования в образовательном процессе образовательных организаций, реализующих программы среднего профессионального образования по специальности "Инфокоммуникационные сети и системы связи" / Е. Л. Новикова. - Москва: Академия, 2018. – 192 с.

6. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

7. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябовд.Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2016. – 363 с.

8. Томаси У. Электронные системы связи.- М.: Техносфера, 2016. -1360с.

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

1. Бабаш, А.В. Криптографические методы защиты информации: учебник / Бабаш А.В., Баранова Е.К. — Москва: КноРус, 2019. — 189 с. — URL: https://book.ru/book/933943 (дата обращения: 01.11.2019). — Текст: электронный.

2. Баранова, Е.К. Криптографические методы защиты информации. Лабораторный практикум +CD: учебное пособие / Баранова Е.К., Бабаш А.В. — Москва: КноРус, 2017. — 196 с. — URL: https://book.ru/book/920017 (дата обращения: 01.11.2019). — Текст: электронный

3. Голиков А.М. Кодирование в телекоммуникационных системах [Электронный ресурс]: учебное пособие Курс лекций, компьютерный практикум, задание на самостоятельную работу / А.М. Голиков. - Электрон. текстовые данные. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. - 338 с.- Режим доступа: http://www.iprbookshop.ru/72111.html

4. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс]: учебное пособие / А.О. Горбенко. - Электрон. текстовые данные. — СПб.: Интермедия, 2017. - 335 с. - Режим доступа: http://www.iprbookshop.ru/66797.html

5. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

6. Креопалов, В. В. Технические средства и методы защиты информации: учебное пособие / В. В. Креопалов. — М.: Евразийский открытый институт, 2011. — 278 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/10871.html (дата обращения: 01.11.2019). — Режим доступа: для авторизир. пользователей

7. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

8. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/80290.html (дата обращения: 05.11.2019). — Режим доступа: для авторизир. пользователей

3.2.3. Дополнительные источники

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

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

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

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

8. 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».

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

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

12. 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.

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

14. 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.

15. 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.

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

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

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

19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

20. Руководящий документ. Геоинформационные системы. Защита информации

от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

21. 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.

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

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

38. 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.

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

40. 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.

41. 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.

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

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

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

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

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

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС.	**Практический опыт:** установки, настройки специализированного оборудования криптографической защиты информации	Экспертное наблюдение Экзамен
	Умения: производить установку и настройку типовых программно-аппаратных средств защиты информации	Экспертное наблюдение Экзамен
	Знания: – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах	Экспертное наблюдение Экзамен
ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	**Практический опыт:** – установки, настройки специализированного оборудования криптографической защиты информации – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации	Экспертное наблюдение Экзамен
	Умения: производить установку и настройку типовых программно-аппаратных средств защиты информации	Экспертное наблюдение Экзамен
	Знания: – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения	Экспертное наблюдение Экзамен

	программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах – основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы	
ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС.	**Практический опыт:** – определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации; – установки, настройки специализированного оборудования криптографической защиты информации – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации	Экспертное наблюдение Экзамен
	Умения: – выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;	Экспертное наблюдение Экзамен
	– Знания: – типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы	Экспертное наблюдение Экзамен

	идентификации и аутентификации в телекоммуникационных системах; – основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы – основные понятия криптографии и типовые криптографические методы защиты информации.	
ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение запасного имущества	**Практический опыт:** – установки, настройки специализированного оборудования криптографической защиты информации – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации	Экспертное наблюдение Экзамен
	Умения: пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации	Экспертное наблюдение Экзамен
	Знания: – типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах – основные способы противодействия	Экспертное наблюдение Экзамен

	несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	**Умения:** – обоснованная постановка цели, выбора и применения методов и способов решения профессиональных задач; – адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Экспертное наблюдение Экзамен
	Знания: – различных способов решения поставленной задачи	Экспертное наблюдение Экзамен
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	**Умения:** – использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Экспертное наблюдение Экзамен
	Знания: – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	**Умения:** – демонстрация ответственности за принятые решения; – обоснованность самоанализа и коррекция результатов собственной работы	Экспертное наблюдение Экзамен
	Знания:	Экспертное наблюдение

	– методов самоанализа и коррекции результатов собственной работы	Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	**Умения:** – взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; – обоснованность анализа работы членов команды (подчиненных)	Экспертное наблюдение Экзамен
	Знания: – методик анализа работы членов команды	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	**Умения:** – эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	Экспертное наблюдение Экзамен
	Знания: – основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	**Умения:** – эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	Экспертное наблюдение Экзамен
	Знания: – основные понятия криптографии и типовые криптографические методы защиты информации.	Экспертное наблюдение Экзамен