Федеральное государственное образовательное бюджетное

учреждение высшего образования

«Финансовый университет при Правительстве Российской Федерации»

(Финансовый университет)

Колледж информатики и программирования

СОГЛАСОВАНО

Общество с ограниченной ответственностью «Русбитех-Астра»
Директор департамента регионального развития

_____ А.Б. Солдатов

«24» мая 2024 г.

УТВЕРЖДАЮ

Заместитель директора по учебной работе

_____ Н.Ю. Долгова

«10» июня 2024 г.

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

Москва 2024 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

Разработчики:

Маринич А.Л., преподаватель первой квалификационной категории Колледжа информатики и программирования

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии «Обеспечение информационной безопасности автоматизированных систем»

Протокол от «16» мая 2024 г. №10

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

1. Общая характеристика рабочей программы профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности: защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

1.1.1. Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных 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.

1.1.2. Перечень профессиональных компетенций

Код	Профессиональны компетенции
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.

1.1.3. В результате освоения профессионального модуля студент 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; *Анализ защищенности информационной инфраструктуры значимых объектов критической информационной инфраструктуры* *Участие в формировании требований к назначению, структуре и конфигурации создаваемой значимых объектов критической информационной инфраструктуры* *Участие в разработке модели угроз безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры* *Обоснование перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации значимых объектов критической информационной инфраструктуры* *Участие в определении комплекса мер для защиты информации значимых объектов критической информационной инфраструктуры* *Участие в формировании разделов технических заданий на создание систем безопасности значимых объектов критической информационной инфраструктуры* *Участие в определении правил и процедур защиты информации при выводе значимых объектов критической информационной инфраструктуры объектов информатизации из эксплуатации* *Анализ технической документации информационной инфраструктуры значимых объектов критической информационной инфраструктуры* *Подготовка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации* *Подготовка документов, определяющих правила и процедуры управления конфигурацией системой безопасности значимых объектов критической информационной инфраструктуры* *Подготовка документов, определяющих правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в автоматизированной системе* *Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ* *Установка обновлений программного обеспечения значимых объектов критической информационной инфраструктуры*

	Управление полномочиями пользователей значимых объектов критической информационной инфраструктуры *Обнаружение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры* *Устранение неисправностей в работе системы безопасности значимых объектов критической информационной инфраструктуры* *Устранение инцидентов, возникших в процессе эксплуатации значимых объектов критической информационной инфраструктуры* *Осуществление автономной наладки технических и программных средств системы защиты информации значимых объектов критической информационной инфраструктуры;* *Участие в разработке организационных и технических мероприятий по защите объектов КИИ;* *Установка, настройка и применение современных средств защиты информации, обрабатываемой объектами КИИ;* *Работа с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов КИИ, в том числе зарубежными информационными ресурсами* *Эксплуатация системы безопасности значимого объекта КИИ* *Участие в восстановлении после сбоев и отказов программного обеспечения значимых объектов критической информационной инфраструктуры**
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; *применять нормативные правовые акты, определяющие требования к обеспечению информационной безопасности объекта критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;* *определять информационную инфраструктуру и информационные ресурсы значимых объектов критической информационной инфраструктуры, подлежащие защите;* *классифицировать и оценивать угрозы безопасности информации для значимых объектов критической информационной инфраструктуры на предприятии (объекте);*

	определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта КИИ; *определять требования к параметрам настройки программных и программно-аппаратных средств, наличия средств защиты информации, обеспечивающих реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации;* *оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;* *участвовать в выборе мер защиты информации, подлежащие реализации в системе защиты информации значимых объектов критической информационной инфраструктуры;* *принимать участие в выборе программно-аппаратные средств защиты информации для использования их в составе значимых объектов критической информационной инфраструктуры критической информационной инфраструктуры объектов;* *участвовать в определении комплекса мер для обеспечения безопасности информационной безопасности в значимых объектах критической информационной инфраструктуры;* *выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации* *применять нормативные документы по противодействию технической разведке;* *планировать политику безопасности программных компонентов значимых объектах критической информационной инфраструктуры* *участвовать в разработке политики безопасности информации значимых объектов критической информационной инфраструктуры;* *конфигурировать параметры средств защиты информации и системы безопасности значимых объектов критической информационной инфраструктуры* *определять параметры настройки программного обеспечения системы защиты информации значимых объектов критической информационной инфраструктуры;* *использовать криптографические методы и средства защиты информации в значимых объектах критической информационной инфраструктуры;* *регистрировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры* *анализировать события, связанные с защитой информации в значимых объектах критической информационной инфраструктуры;* *использовать программные средства для архивирования информации;* *использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации;* *применять типовые программные средства резервирования и восстановления информации в значимых объектах критической информационной инфраструктуры;*

	применять средства обеспечения отказоустойчивости значимых объектов критической информационной инфраструктуры *определять источники и причины возникновения инцидентов* *оценивать последствия выявленных инцидентов* *обнаруживать нарушения правил разграничения доступа* *устранять нарушения правил разграничения доступа**
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; *Законодательство Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры* *Нормативные правовые акты в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.* *Основные методические и руководящие документы по защите информации в областях, относящихся к областям функционирования значимых объектов критической информационной инфраструктуры* *Национальные, межгосударственные и международные стандарты в области защиты информации (информационной безопасности)* *Модель угроз информационной безопасности, модель нарушителя информационной безопасности на объекте информатизации* *Эксплуатационная и проектная документация на информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, обеспечивающие функционирование объекта информатизации* *Основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;* *Основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ;* *Принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования;* *Процедура категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ;* *Процедура подготовки и направления в ФСТЭК России сведений о результатах присвоения объекту КИИ одной из категорий значимости*

	либо об отсутствии необходимости присвоения ему одной из таких категорий *Основные принципы выявления наличия критических процессов у субъектов КИИ* *Основные принципы выявления объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;* *Общие требования по обеспечению безопасности значимых объектов КИИ;* *Общие требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования;* *Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ* *Основные угрозы безопасности информации и модели нарушителя в значимых объектах критической информационной инфраструктуры* *Регламент информирования персонала значимых объектов критической информационной инфраструктуры* *Регламент учета выявленных инцидентов* *Регламент устранения инцидентов* *Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры* *Процедуры по архивированию информации, обрабатываемой на значимых объектах критической информационной инфраструктуры* *Регламент значимых объектов критической информационной инфраструктуры по уничтожению информации и машинных носителей информации* *Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационной инфраструктуры и систем безопасности значимых объектов критической информационной инфраструктуры* *Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ;* *Цели, задачи, основные принципы организации государственного контроля в области обеспечения безопасности значимых объектов КИИ;* *Порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов КИИ* *Критерии оценки защищенности значимых объектов критической информационной инфраструктуры* *Технические средства контроля эффективности мер защиты информации* *Содержание и порядок деятельности персонала по эксплуатации защищенных значимых объектов критической информационной инфраструктуры и систем безопасности значимых объектов критической информационной инфраструктуры* *Основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения защиты информации в значимых объектах критической информационной инфраструктуры**

*вариативная часть

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: 746 часов, в том числе в форме практической подготовки 746 часов
Из них на освоение МДК – 482 часов:
в том числе: самостоятельная работа -36 часов,
курсовой проект (работа) в составе МДК.02.01 и МДК.02.02 -30 часов.

Практики, в том числе учебная -108 час.
производственную -144час.
Экзамен по модулю- 12 часов

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.							Самостоятельная работа
			В т.ч. в форме практической подготовки			Обучение по МДК		Практики		
				всего, часов	Промежуточная аттестация	Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная	
ПК 2.1-2.3 ОК.01-04, ОК.09,10	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	358	358	284	18	80	20	54		20
ПК 2.1-2.3 ОК.01-04, ОК.09,10	Раздел 2. Криптографическая защита информации	232	232	162	-	44	10	54		16
ПК 2.1-2.3	Производственная практика	144	144						144	

ОК.01-04, ОК 09,10										
	Экзамен по модулю	12	12	12	12					
	Всего:	746	746	458	30	124	30	108	144	36

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 студентов, курсовой проект (работ)	Объем часов
1	2	3
Раздел 1.ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**358**
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**304**
Тема 1.1. Обеспечение безопасности операционных систем	Содержание	46
	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. Windows 7. Windows8. Linux. QNX и другие операционные системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации Пароли. PIN-коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи. Программно-аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон –Замок системный администратор. Изучение настроек системного администратора АПМДЗ.	30

	АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог.	
	В том числе практических и лабораторных занятий:	16
	1. Практическое занятие «Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя»	2
	2.Практическое занятие «Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита»	2
	3. Практическое занятие «Настройка изолированной среды»	2
	4. Практическое занятие «АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды»	4
	5. Практическое занятие «Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация»	2
	6. Практическое занятие «Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование»	2
	7. Практическое занятие «Восстановление информации типовыми средствами Программы восстановление информации»	2
Тема1.2. Технологии разграничения доступа	Содержание	52
	Архитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Server2016. Возможности администратора. Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда.	42

	Способы организации. Методы применения. ActiveDirectory. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	
	В том числе практических и лабораторных занятий:	10
	1. Практическое занятие «Программы надежного удаления информации»	2
	2. Практическое занятие «Архивирование информации»	2
	3. Практическое занятие «Программные средства резервного копирования. Настройка RAID-массивов»	2
	4. Практическое занятие «Инсайдерская информация. Программы сбора информации о ПК»	2
	5. Практическое занятие «Настройка межсетевого экрана».	2
Тема 1.3. Обеспечение информационной безопасности сетей.	Содержание	62
	Проблемы информационной безопасности сетей.	26

Основы технологии виртуальных защищенных сетей VPN	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. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом. Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	
	В том числе практических и лабораторных занятий:	36
	1. Практическое занятие «Основные действия с виртуальной машиной»	2
	2. Практическое занятие «Работа с контрольными точками»	2
	3. Практическое занятие «Использование внешних устройств»	2
	4. Практическое занятие «Работа с локальным хранилищем сертификатов в ОС WINDOWS»	2
	5. Практическое занятие «Установка и настройка ПО eTokenPKIClient»	2
	6. Практическое занятие «Настройка ПО eTokenPKIClient с помощью групповых политик»	2
	7. Практическое занятие «Развертывание TMS в среде Active Directory»	2

	8. Практическое занятие «Настройка TMS в среде Active Directory»	2
	9. Практическое занятие «Настройка политик TMS»	2
	10. Практическое занятие «Настройка использования виртуального токена»	2
	11. Практическое занятие «Использование токена на рабочем месте администратора»	2
	12. Практическое занятие «Установка и настройка СКЗИ «КриптоПроCSP»	2
	13. Практическое занятие «Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP»	2
	14. Практическое занятие «Применение SecretDisk4»	2
	15. Практическое занятие «Применение SecretDisk Server NG»	2
	16. Практическое занятие «Изучение основных возможностей ПО VipNetClient»	2
	17. Практическое занятие «Изучение настроек ПО VipNetClient»	2
	18. Практическое занятие «Изучение возможностей ПО Деловая почта»	2
Тема 1.4. Технологии обнаружения вторжений	Содержание	24
	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. 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. Технологии защиты от вирусов.	20

	Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусовЖизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	
	В том числе практических и лабораторных занятий:	4
	1. Практическое занятие «Изучение средств обнаружения атак»	2
	2.Практическое занятие «Изучение антивирусных продуктов»	2
Тема 1.5. Методы управления средствами защиты	Содержание	12
	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	12
	В том числе практических и лабораторных занятий	-
Тема 1.6 Обеспечение безопасности значимых объектов критической информационной инфраструктуры *	Содержание	50
	Правовые основы обеспечения безопасности КИИ Российской Федерации	6
	Угрозы безопасности информации, обрабатываемой на объектах КИИ	4
	Категорирование объектов КИИ	6
	Требования по обеспечению безопасности значимых объектов КИИ	6
	Система безопасности значимого объекта КИИ Обеспечение бесперебойной эксплуатации значимых объектов КИИ	6
	Контроль за обеспечением безопасности значимого объекта КИИ	8

	В том числе практических и лабораторных занятий:	14
	1.Практическое занятие «Анализ нормативных документов для объектов КИИ»	2
	2.Практическое занятие «Разработка регламента управления инцидентами и плана реагирования на компьютерные инциденты»	2
	3.Практическое занятие «Разработка технического задания на создание системы безопасности значимого объекта КИИ»	2
	4.Практическое занятие «Разработка программы и методики испытаний средств защиты информации на соответствие требованиям по безопасности»	2
	5.Практическое занятие Разработка модели угроз безопасности информации значимого объекта КИИ	2
	6.Практическое занятие «Проведения анализа защищенности значимого объекта КИИ на соответствие требованиям по обеспечению безопасности»	2
	7.Практическое занятие «Работа с ПАК для подключения к ГосСОПКА»	2
	8.Практическое занятие «Разработка регламента аудита безопасности объекта КИИ»	2
Тематика курсовых работ (комплексная курсовая работа по двум разделам ПМ) 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)		**20**

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.	
Примерная тематика внеаудиторной самостоятельной работы при изучении раздела	**20**
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. 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. Инсталяция. 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. Тунелирование. 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.3.сыМЭ. ТребованияФСТЭКкМЭ.куюдокументациюнаоборудованиеИТКС.	

23.Функционирование системы управления средствами защиты. 24.Аудит безопасности информационной системы.		
Промежуточная аттестация в форме в форме экзамена МДК.02.01		**18**
Учебная практика по 1 Разделу Виды работ: 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.		**54**
Раздел 2. ПМ.02 Криптографическая защита информации		**232**
МДК 02.02.Криптографическая защита информации		**178**
	Содержание	48

Тема 2.1. Основы криптографических методов защиты информации	Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста . Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	32
	В том числе практических и лабораторных занятий:	16
	1. Практическое занятие «Стеганографические методы скрытия информации»	2
	2. Практическое занятие «Бинарная арифметика. Модульная арифметика»	2
	3. Практическое занятие «Применение методов шифрования перестановкой»	2
	4. Практическое занятие «Применение методов шифрования заменой»	2
	5. Практическое занятие «Применение методов шифрования многоалфавитной замены»	2
	6. Практическое занятие «Криптоанализ методов перестановки»	2
	7. Практическое занятие «Криптоанализ методов замены»	2

	8. Практическое занятие «Компьютерное шифрование»	2
Тема 2.2. Современные стандарты шифрования	Содержание	30
	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. Российские стандарты симметричного шифрования . Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	26
	В том числе практических и лабораторных занятий:	4
	1. Практическое занятие «Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа»	2
	2. Практическое занятие «Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители»	2
	Содержание	56

Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	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. 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. Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/M1ME . Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети Защита информации в сетях организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. Защита информации в сетях сотовой связи. A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.	32
	В том числе практических и лабораторных занятий:	24
	1. Практическое занятие «Разработка хэш-функции»	2

	2. Практическое занятие «Разработка схемы простого пароля»	2
	3. Практическое занятие «Разработка схемы динамического пароля»	2
	4. Практическое занятие «Сертификаты открытого ключа»	2
	5. Практическое занятие «Настройка и администрирование токена»	2
	6. Практическое занятие «Настройка сервисов Рутокен-PinPad»	2
	7. Практическое занятие «Настройка сервисов Рутокен-ЭЦП»	2
	8. Практическое занятие «Настройка сервисов Рутокен–Bluetooth»	2
	9. Практическое занятие «Настройка сервисов Рутокен–S»	2
	10 Практическое занятие «Разработка алгоритма PGP»	2
	11. Практическое занятие «Изучение протоколов SSL, TLS, IPSec»	2
	12. Практическое занятие «Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2»	2
*Тема 2.1 Защита АРМ пользователя на основе технологии ViPNet**	Содержание	16
	VPN и персональный сетевой экран. Криптопровайдер. Настройка VPN и персонального сетевого экрана Установка и настройка криптопровайдера, р2абота с сертификатами Установка прямого взаимодействия по каналу MFTP Настройка автопроцессинга в программе ViPNet Деловая почта	16
	В том числе практических и лабораторных занятий	-
Промежуточная аттестация в форме в форме дифференцированного зачета по МДК.02.02		**2**

Тематика курсовых проектов работ (комплексная работа по двум разделам ПМ) 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.	**10**
Примерная тематика внеаудиторной самостоятельной работы по разделу: Изучение новых технологий хранения информации. Статистика и анализ крупных утечек информации за год. Поиск информации о новых видах атак на информационную систему. Обзор современных программных и программно-аппаратных средств защиты. 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.	**16**

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.	
Учебная практика раздела 2 Виды работ Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции Составление алгоритма шифра Подключение, установка драйверов, настройка программных средств шифрования Криптон. Администрирование программных средств шифрования Криптон Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. Администрирование аппаратных средств шифрования Криптон.	**54**
Производственная практика 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. Проведение инструктажа по технике безопасности. 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	**144**

Промежуточная аттестация в форме экзамена по модулю	**12**
Всего	**746**

**вариативная часть*

3. Условия реализации рабочей программы профессионального модуля

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:
Лаборатория Программных и программно-аппаратных средств защиты информации
Помещение для самостоятельной работы

3.2. Информационное обеспечение реализации программы
Основные печатные и электронные издания

1. 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, 2024. – 363 с.

2.Томаси У. Электронные системы связи.- М.: Техносфера, 2020. -1360с.

3.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2024. – 184 с.

Электронные издания (электронные ресурсы)

Интернет-ресурсы:

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

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

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

Дополнительные источники

Дополнительные источники:

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

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

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

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

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

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

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

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».

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

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.

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

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.

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

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.

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.

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

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

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

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

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

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.

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

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

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

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

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

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

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

ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

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

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

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

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

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

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

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

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

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.

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

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.

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.

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

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

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

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

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

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

4. Контроль и оценка результатов освоения профессионального модуля

Код и наименование профессиональных и общих компетенции, 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.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение за выполнением практических работ Дифференцированный зачет Экзамен Защита курсовой работы Экзамен по модулю

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	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно-	Экспертное наблюдение за выполнением практических работ Дифференцированный зачет Экзамен Защита курсовой работы Экзамен по модулю
ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты	Экспертное наблюдение за выполнением практических работ Дифференцированный зачет Экзамен Защита курсовой работы
ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты	Экспертное наблюдение за выполнением практических работ Дифференцированный зачет Экзамен Защита курсовой работы
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	Экспертное наблюдение

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством,	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение