МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)
Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 009b47d8b89b08d0f6
Владелец: Киричек Руслан Валентинович
Действителен с 13.02.2023 по 12.02.2028

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
_____ 2023 г.

Регистрационный № 11.09.23/167

РАБОЧАЯ ПРОГРАММА

ПМ.02. ЗАЩИТА ИНФОРМАЦИИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ПРОГРАМНЫХ И ПРОГРАММНО-АППАРАТНЫХ В ТОМ ЧИСЛЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

(наименование профессионального модуля)

по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2023

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.02) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 30 марта 2023 г., протокол № 3.

Составитель:
Преподаватель _____ Н.В.Кривоносова
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 9 (Информационной безопасности телекоммуникационных систем)
1 февраля 2023 г., протокол № 6

Председатель предметной (цикловой) комиссии: _____ Н.В.Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
8 февраля 2023 г., протокол № 3

Заместитель директора по учебной работе колледжа СПб ГУТ _____ Н.В. Калинина
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ _____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО

Директор департамента ОКОД _____ С.И. Ивасишин
(подпись)

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 рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 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 «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 и личностных результатов реализации программы воспитания

Код	Наименование общих компетенций и личностных результатов
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 языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28	

1.2.2 Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
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 информационно-телекоммуникационных системах и сетях
ПК 2.3	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями

1.2.3 В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных в том числе криптографических средств защиты информации в оборудовании ИТКС; – поддержании бесперебойной работы программных и программно-аппаратных в том числе криптографических средств защиты информации в ИТКС; – защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.
уметь	– 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; – проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; – 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 программных и программно-аппаратных, в том числе криптографических средств защиты информации.
знать	– возможные угрозы безопасности информации в ИТКС; – способы защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на неё; – типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

	– криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; – порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; – организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; – порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографических средств защиты информации.

1.2 Количество часов, отводимое на освоение профессионального модуля

Всего часов: **776 часов.**

Из них на освоение МДК**:**

МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты- **292 часа;**

МДК.02.02. Криптографическая защита информации - **178 часов;**

На практики учебную и производственную - **288 часов.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	**Объем профессионального модуля, час.**								
		Суммарный объем нагрузки, час.	В т.ч. в форме практической подготовки	Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа	Промежуточная аттестация
				Обучение по МДК, в час.			Практики			
				Всего	Лабораторные работы и практические занятия	в т.ч., курсовая работа (проект)	Учебная	Производственная (по профилю специальности)		
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	**292**	96	**236**	66	30	**72**		**52**	**4**
ПК 2.1-2.3 ОК 01-04, ОК 09,10	Раздел 2. Криптографическая защита информации	**178**	44	**156**	44	-	36		**18**	**4**
Учебная практика		**108**	108				108			
Производственная практика		**180**	180					180		
Промежуточная аттестация		**18**								18
Всего:		**776**	428	**392**	110	30	**108**	**180**	**70**	**26**

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 обучающихся, курсовая работ (проект)	Объем часов
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			**292**
МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты			292
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание учебного материала**		30
	1	**Занятие 1. Проблемы обеспечения безопасности операционных систем.** Угрозы безопасности ОС. Взаимосвязь понятий защищенность, уязвимость, угроза, атака, ущерб. Угрозы безопасности ОС: классификация угроз безопасности, типичные атаки на ОС.	
	2	**Занятие 2. Подходы к построению защищенных ОС** Административные меры защиты. Адекватная политика безопасности. Стандарты защищенности и адекватная политика безопасности. Примеры защищенных ОС.	
	3	**Занятие 3. Типовая архитектура подсистемы защиты операционной системы.** Основные функции подсистемы защиты операционной системы. Разграничение доступа к объектам операционной системы: правила разграничения доступа, разрешительная система доступа.	
	4	**Занятие 4. Идентификация, аутентификация и авторизация субъектов доступа** Соотношение идентификации, аутентификации и авторизации, способы и виды аутентификации, идентификация и аутентификация с помощью имени и пароля (методы подбора пароля, защита от компрометации пароля). Идентификация и аутентификация с помощью внешних носителей ключевой информации. Идентификация и аутентификация с помощью биометрических характеристик пользователей.	
	5	**Занятие 5. Аудит безопасности ОС** Цели аудита, требования к аудиту, политика аудита.	
	6	**Занятие 6. Процессы-серверы в Windows** Подходы к выполнению привилегированных действий в Windows (временное получение дополнительных полномочий (полномочий другого пользователя), обращение к услугам процесса-сервера), процесс-серверы в Windows, олицетворение пользователя.	

	7	**Занятие 7. Аудит и обнаружение атак в Windows** Журнал аудита, политика аудита, типы регистрируемых событий, использование информации из журнала аудита для анализа (анализ попыток регистрации, анализ доступа к объектам, анализ выполняющихся задач (отслеживание процессов). **А**нализ использования привилегий, анализ событий с учетными записями, анализ изменения политик). Требования к политике аудита. Администраторы и аудиторы (разделение).	
	8	**Занятие 8. Внедрение вредоносных программ через реестр и планировщик заданий Windows** Структура и расположение реестра, ключи автозагрузки для внедрения потенциально опасных программ (8 случаев). Планировщик заданий в Windows, средства контроля автозагрузки.	
	9	**Занятие 9. Политики ИПС, SRP и Applocker** Подходы к созданию изолированной программной среды до Windows, политика ограниченного использования программ (SRP). **П**олитика Applocker и ее сравнение с SRP.	
	10	**Занятие 10. Идентификация, аутентификация и авторизация пользователей в Windows**. Механизм идентификации, аутентификации и авторизации в Windows: структура механизма идентификации и аутентификации, виды (типы) входа в систему, идентификация и аутентификация с помощью msv1_0(NTLM) - верхний, средний и нижний уровни, идентификация и аутентификация с помощью Kerberos v.5. Провайдеры сетевой аутентификации, параметры идентификации и аутентификации в Windows, Credential Provider'ы (поставщики учетных данных) в ОС Windows	
	11	**Занятие 11. 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. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ	
	12	**Занятие 12. Защита в ОС Unix (Linux)** Компоненты подсистемы защиты в Unix (Linux). Объекты и субъекты доступа в в Unix (Linux). Разграничение доступа в Unix (Linux). Встроенные средства шифрования Unix (Linux). Аудит и обнаружение атак в ОС Unix (Linux).	
	13	**Занятие 13. Защита в ОС Unix (Linux)** Идентификация, аутентификация и авторизация пользователей в ОС Unix (Linux). Процессы-серверы в ОС Unix (Linux). Внедрение вредоносных программ в ОС Unix (Linux). Особенности защиты в серверных версиях ОС Unix (Linux).	
	14	**Занятие 14. Безопасность мобильных ОС** Актуальные угрозы безопасности мобильных ОС. Особенности защиты в ОС Android: -	

		аутентификация и технология Smart Lock, - цифровые подписи приложений, - полномочия, - ограничения (полномочий, API, на доступ к информации и устройствам, на работу в сети, на запуск приложений, на доступ к памяти, - шифрование данных.	
	15	**Занятие 15. Безопасность мобильных ОС** Особенности защиты в ОС Android: - доверенная среда исполнения, - доверенная загрузка, - защита от срыва стека, - технология SELinux, - технология Seccomp, - технология SafetyNet.	
	Лабораторные работы		
	1	**Занятие 16.** Средства идентификации аутентификации операционных систем	**8**
	2	**Занятие 17.** Настройка локальной политики безопасности операционной системы. Политика паролей. Политики учетных записей.	
	3	**Занятие 18.** Назначение прав пользователя.	
	4	**Занятие 19.** Настройка изолированной среды	
	Практические занятия		
	1	**Занятие 20.** Параметры безопасности. Политика аудита	10
	2	**Занятие 21.** АПМДЗ Криптон: инициализация системного администратора, инициализация пользователя, проверка целостности среды	
	3	**Занятие 22.** Аппаратные средства шифрования Криптон: настройка, эксплуатация	
	4	**Занятие 23.** Программные средства шифрования. Защищенные контейнеры.	
	5	**Занятие 24.** Восстановление информации типовыми средствами	
Тема 1.2. Технологии разграничения доступа	**Содержание учебного материала**		**36**
	1	**Занятие 25. Политика и модели безопасности в компьютерных системах** Понятие политики безопасности. Модель безопасности как формализованное выражение политики безопасности. Модель безопасности как основа архитектурных, схемотехнических и программно-алгоритмических решений при создании защищенных КС, анализа систем защиты информации в КС. Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временна́я, маршрутная.	
	2	**Занятие 26. Программно-техническая структура компьютерной системы в контексте безопасности** Понятие и функции монитора (ядра) безопасности. Требования к монитору безопасности. Монитор безопасности объектов (монитор ссылок) и монитор безопасности субъектов (монитор приложений).	
	3	**Занятие 27. Модели безопасности на основе дискреционной политики**	

		Общая характеристика политики дискреционного доступа. Тройки доступа: субъектоперация-объект. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа. Модели разграничения доступа на основе матрицы доступа.	
	4	**Занятие 28. Дискреционная модель** Принудительный и добровольный принцип управления доступом. Администраторы системы и владельцы объектов. Привилегии и предоставление (распространение) прав доступа. Способы организации информационной структуры матрицы доступа — централизованная структура (системные таблицы доступа в реляционных СУБД, биты доступа в ОС UNIX) и децентрализованная структура (списки доступа объектов в ОС Windows).	
	5	**Занятие 29. Модели безопасности на основе мандатной политики** Общая характеристика политики мандатного (полномочного) доступа. Парадигма градуированного доверия пользователям (субъектам доступа) и градуированной степени конфиденциальности данных (объектов доступа). Уровни безопасности субъектов и объектов доступа. Правила безопасного мандатного доступа — запрет чтения вверх (NRU) и запрет записи вниз (NWD). Рефрексивность, антисимметричность и транзитивность отношений доступа. Функция уровня безопасности субъектов и объектов доступа. Решетка уровней безопасности. Классы безопасных информационных потоков и матрица доступа.	
	6	**Занятие 30. Модели безопасности на основе тематической политики** Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств. Критерии безопасности информационных потоков в системах тематического разграничения доступа. Тематические решетки на основе классификационных множеств. Решетка подмножеств множества тематических рубрик при дескрипторной классификации. Тематическая решетка на корневом дереве рубрикатора при монорубрицированной иерархической классификации и ее изоморфный вариант в виде решетки листовых подмножеств.	
	7	**Занятие 31. Модели безопасности на основе ролевой политики** Общая характеристика политики ролевого (типизованного) доступа. Роль как типовой субъект доступа (функционально обособленное агрегирование прав доступа и полномочий выполнения процедур над данными). Две фазы организации ролевого доступа — создание ролей как типовых субъектов доступа с наделением их правами (полномочиями) доступа на основе дискреционной, мандатной, тематической или иной политики безопасности и назначение ролей пользователям. Сеансовый характер функционирования компьютерной системы с ролевым доступом. Сеансовая	

		авторизация пользователя с одной или группой назначенных ему в системе ролей и доступ к объектам системы в соответствующей (соответствующих) роли (ролях). Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями.	
	8	**Занятие 32. Модели и механизмы обеспечения целостности данных** Понятие целостности данных и общая характеристика методов и механизмов обеспечения целостности данных. Дискреционная модель обеспечения целостности данных Кларка-Вильсона. Объекты, требующие контроля целостности (constrained data items), процедуры проверки целостности (integrity verification procedures), корректно сформированные транзакции (не нарушающие ограничения целостности), тройки "субъект-транзакция-объект". Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных (запрет "чтения вниз", запрет "записи вверх") как инверсия правилам мандатного доступа, не нарушающим конфиденциальность данных (в модели Белла-Лападулы).	
	9	**Занятие 33. Методы и технологии обеспечения доступности (сохранности) данных** Резервирование, архивирование и журнализация данных. Организационные, технологические и программно-технические принципы политики резервирования и архивирования БД. Оперативное сохранение (журнализация) изменений данных. Восстановление данных из архивной копии и по журналу изменений данных. Синхронная и асинхронная журнализация. Полное и инкрементное сохранение измененных данных. Сценарии архивирования/журнализации.	
	10	**Занятие 34. Методы и технологии обеспечения доступности (сохранности) данных** Системы реального времени. "Горячее" резервирование. Главный/резервный серверы. "Прозрачность" для приложений. Автоматическое переключение серверов, "поднятие" "упавшего" сервера. Системы репликации данных. Обеспечение непрерывности согласованного состояния данных, синхронная и асинхронная репликации. Программно-техническая структура систем репликации данных. Обеспечение непрерывности согласованного состояния структуры данных, системы с "главной" и частичными репликами.	
	11	**Занятие 35. Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем** Понятие измерения величин и оценки объектов как отображения множеств с отношениями. Процесс измерения (оценки) и шкала измерения (оценки). Точные измерения и измерения с погрешностями. Типы шкал (шкалирования) – номинальные шкалы, порядковые (ранговые) шкалы, шкалы интервалов, шкалы отношений, шкалы разностей и абсолютные шкалы.	

		Многомерное оценивание сложных объектов и его целевые разновидности – определение сравнительного предпочтения объектов, определение сходства и различия объектов, типизация (классификация и группирование) объектов. Оценка защищенности (безопасности) компьютерных систем как задача многомерного шкалирования свойств КС в аспекте безопасности. Иерархический (древовидный) характер системы критериев анализа КС (параметров, свойств, функций), обеспечивающих составляющие безопасности (конфиденциальность, целостность и доступность информации). Порядковое (ранговое) шкалирование компьютерных систем в аспекте безопасности на основе группирования (классификации) в пространстве шкалирования первичных факторов оценки. Примеры многомерных номинально-ранговых систем оценки защищенности компьютерных систем, закрепленные в стандартах безопасности.	
	12	**Занятие 36. Разграничение доступа в ОС Windows.** Методы доступа к объектам в Windows. Права доступа к объектам в Windows. Привилегии субъектов в Windows. Разрешения NTFS для файлов и папок. Маркер доступа (AC) пользователя. Дескриптор защиты (SD) объекта: структура дескриптора защиты, списки управления доступом (DACL и SACL), маска прав в ACE, флаги в ACE - их назначение, отличие от флагов в SD, использование при наследовании.	
	13	**Занятие 37. Разграничение доступа в ОС Windows** Идентификатор безопасности (SID) пользователя. Проверка прав доступа субъекта к объекту: общий порядок проверки SRM прав доступа субъектов к объектам, два варианта (функции) проверки прав доступа субъекта к объекту, примеры проверки прав доступа при обращении субъекта к объекту. Назначение атрибутов защиты (DACL) создаваемым (новым) объектам в Windows. Защита от несанкционированных действий администратора.	
	14	**Занятие 38. Аудит безопасности операционной системы** Методы проведения контрольных проверочных мероприятий. Программные средства аудита	
	15	**Занятие 39. Межсетевые экраны** Понятие межсетевого экрана. Виды МЭ. Функции межсетевых экранов. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов	
	16	**Занятие 40. Защита информации на сетевом уровне** Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов	
	17	**Занятие 41. Политика межсетевого взаимодействия.** Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ.	

		Тестирование межсетевых экранов	
	18	**Занятие 42. Требования показателей тестирования МЭ** Классы МЭ. Требования ФСТЭК к МЭ	
	Практические занятия		
	6	**Занятие 43.** Программы надежного удаления информации	**10**
	7	**Занятие 44.** Архивирование информации	
	8	**Занятие 45.** Программные средства резервного копирования. Настройка RAID-массивов	
	9	**Занятие 46.** Инсайдерская информация. Программы сбора информации о ПК	
	10	**Занятие 47.** Настройка межсетевого экрана	
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание учебного материала**		**26**
	1	**Занятие 48. Сетевая безопасность** 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	**Занятие 49. Введение в технологию виртуальных частных сетей (VPN).** Виртуальная частная сеть: основные понятия, цели создания, определения, подходы. Основные задачи технологии VPN. Специфика построения VPN. VPN в публичных сетях. Туннелирование в VPN. Протоколы механизма туннелирования.	
	3	**Занятие 50. Схема и политики безопасности VPN.** Схема VPN. Алгоритм работы VPN-агентов. Функции VPN-агентов. Политики безопасности в VPN. Критерии безопасности VPN. Варианты создания VPN (защищённые каналы, частные каналы, промежуточные каналы). Примеры политик безопасности VPN.	
	4	**Занятие 51. Стандартные протоколы создания VPN** Уровни защищённых каналов. Семиуровневая модель взаимодействия открытых систем (OSI). Протоколы защиты данных канального уровня (PPTP, L2F и L2TP). Сравнительный анализ протоколов защиты на канальном уровне.	
	5	**Занятие 52. Защита данных на сетевом уровне** Протокол IPSec. Протоколы туннельного и транспортного режимов. Защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS).	
	6	**Занятие 53. Особенности управления ключевой системой асимметричных криптосистем**. Инфраструктура открытых ключей. Проблемы управления криптографическими ключами.	

		Жизненный цикл ключей. Компрометация ключей. Управление секретными и открытыми ключами. Инфраструктура открытых ключей (ИОК). Модели APKI и PKIX	
	7	**Занятие 54. Сертификация открытых ключей.** Основные подходы к обеспечению безопасности открытых ключей. Содержание метода сертификации открытых ключей. Удостоверяющий центр. Сертификат открытого ключа. Формат сертификации открытого ключа. Аннулирование сертификатов. Модель инфраструктуры открытых ключей. Основные протоколы ИОК согласно модели PKIX. Закон РФ «Об электронной подписи»	
	8	**Занятие 55. Требования к продуктам построения виртуальных частных сетей.** Варианты реализации. Характеристика основных средств построения VPN. Производительность. Управляемость. Совместимость. Поддержка справочной службы. Надёжность защиты и функциональная полнота.	
	9	**Занятие 56. Принципы построения виртуальных частных сетей.** Реализация алгоритмов скоростной криптозащиты. Варианты реализации VPN. Шлюзы и клиенты VPN.	
	10	**Занятие 57. Решения для построения виртуальных частных сетей.** VPN на базе сетевых операционных систем. VPN на базе маршрутизаторов. VPN на базе межсетевых экранов.	
	11	**Занятие 58. Решения для построения виртуальных частных сетей**. VPN на базе специализированного программного обеспечения. VPN на базе аппаратных средств. Виды виртуальных частных сетей.	
	12	**Занятие 59. Характеристика российских продуктов для создания виртуальных частных сетей.** Аппаратно-программный комплекс «Континент». Программные продукты семейства «Застава». Продукты комплекса «VipNet».	
	13	**Занятие 60. Характеристика российских продуктов для создания виртуальных частных сетей.** Семейство продуктов «Net-PRO». Продукты «Шип» и «Игла-2». Сравнительный анализ российских продуктов.	
	Лабораторные работы		
	5	**Занятие 61.** Примеры политик безопасности VPN	26
	6	**Занятие 62.** Протоколы защиты данных канального уровня (PPTP, L2F и L2TP). Сравнительный	

		анализ протоколов защиты на канальном уровне.	
	7	**Занятие 63.** Защита данных на сетевом уровне (Протокол IPSec). Протоколы туннельного и транспортного режимов.	
	8	**Занятие 64.** Защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS)	
	9	**Занятие 65.** Инфраструктура открытых ключей (ИОК). Модели APKI и PKIX	
	10	**Занятие 66.** Сертификат открытого ключа. Формат сертификации открытого ключа. Аннулирование сертификатов	
	11	**Занятие 67.** Реализация алгоритмов скоростной криптозащиты	
	12	**Занятие 68.** VPN на базе сетевых операционных систем	
	13	**Занятие 69.** VPN на базе специализированного программного обеспечения	
	14	**Занятие 70.** VPN на базе аппаратных средств.	
	15	**Занятие 71.** Использование токена на рабочем месте администратора	
	16	**Занятие 72.** Установка и настройка СКЗИ «КриптоПро CSP»	
	17	**Занятие 73.** Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	
Тема 1.4. Технологии обнаружения вторжений	**Содержание учебного материала**		**30**
	1	**Занятие 74. Уязвимости традиционных средств защиты** Уязвимости стека протоколов TCP/IP. Слабости МЭ, и способы его обхода. Уязвимости системы аутентификации и авторизации	
	2	**Занятие 75. Анатомия атаки, этапы осуществления атаки** Классификация уязвимостей. Модель атаки. Этапы реализации атаки. Классификация атак	
	3	**Занятие 76. Задача обнаружения атак** Понятие системы обнаружения атак. Реальные возможности систем обнаружения атак и пределы их возможностей. Схема работы системы обнаружения атак	
	4	**Занятие 77. Основные принципы обнаружения атак** Признаки атак. Источники информации об атаках. Технологии и подходы к обнаружению атак	
	5	**Занятие 78. Обнаружение следов атак** Контроль изменений файлов. Анализ журналов регистрации. Анализ сетевого трафика	
	6	**Занятие 79. Классификация систем обнаружения атак** Системы анализа защищенности. Анализаторы журналов регистрации. Обманные системы. Системы контроля целостности	

	7	**Занятие 80. Выбор системы обнаружения атак** Предварительный анализ. Критерии оценки. Тестирование	
	8	**Занятие 81. Размещение системы обнаружения атак** Размещение сенсоров. Использование сетевых сенсоров коммутируемых сетях. Размещение системы анализа защищенности	
	9	**Занятие 82. Размещение системы контроля целостности** Понятие системы контроля целостности. Методы контроля целостности.	
	10	**Занятие 83. Системы виртуальных ловушек (Honey Pot и Padded Cell)** Понятие ловушек. Виды и способы реализации.	
	11	**Занятие 84. Методы развертывания и эксплуатации СОА** Общие проблемы. Сетевые системы. Узловые системы	
	12	**Занятие 85. Средства анализа защищенности сетевых протоколов и сервисов.** Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности.	
	13	**Занятие 86. 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.	
	14	**Занятие 87. Технологии защиты от вирусов.** Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	
	15	**Занятие 88. Обзор отечественных решений для обнаружения вторжений**	
	Лабораторные работы		**2**
	18	**Занятие 89.** Проектирование стенда для реализации IDS	
	Практические занятия		**10**
	11	**Занятие 90.** Настройка интерфейсов виртуальных машин	
	12	**Занятие 91.** Конфигурация правила для СОВ	
	13	**Занятие 92.** Развертывание открытых списков правил	
	14	**Занятие 93.** Подключение средства мониторинга	
	15	**Занятие 94.** Включение режима блокировки	

Тема 1.5. Методы управления средствами защиты	**Содержание учебного материала**		**18**
	1	**Занятие 95. Методы управления средствами сетевой защиты.** Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты.	
	2	**Занятие 96. 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.	
	3	**Занятие 97. Методы и средства обеспечения информационной безопасности компьютерных систем на административном уровне ИБ.** Обзор справочно-аналитических материалов для принятия управленческих решений на административном уровне. Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий	
	4	**Занятие 98. Методы и средства обеспечения информационной безопасности компьютерных систем на процедурном уровне.** Проектирование, внедрение и эксплуатация в организации ИС и ИКТ на процедурном уровне.	
	5	**Занятие 99. Методы и средства обеспечения информационной безопасности компьютерных систем.** Разработка макетов справочно-аналитических материалов для принятия управленческих решений на основе законодательного уровня ИБ.	
	6	**Занятие 100. Методы и средства обеспечения информационной безопасности компьютерных систем.** Основные методы защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий	
	7	**Занятие 101. Основные программно-технические меры безопасности информации** Постановка и решение схемотехнических задач, связанных с выбором системы элементов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным. Знакомство с методами проектирования, разработки и реализации технического решения в области создания систем защиты информации	
	8	**Занятие 102. Основные программно-технические меры безопасности информации** Протоколирование, аудит, шифрование, контроль целостности, электронная цифровая подпись	
	9	**Занятие 103. Антивирусная защита компьютерных систем**	

		Принципы организации антивирусной защиты информационных систем. Типология вирусов. Достоинства и недостатки эвристических алгоритмов поиска вирусов.	
	Самостоятельная работа обучающихся		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. **Тематика домашних заданий, сообщений, рефератов:** 1. Проблемы обеспечения безопасности операционных систем. 2. Технологии аутентификации. 3. Аутентификация, авторизация и администрирование действий пользователя. 4. Пароли. 5. PIN-коды. 6. Методы надежного составления паролей. 7. Токены. 8. Смарт-карты. 9. Виртуальные ключи. 10. Программно-аппаратные модули доверенной загрузки. 11. АПМДЗ Криптон –Замок системный администратор. 12. Изучение настроек системного администратора АПМДЗ. 13. Сектор НЖМД. 14. Область памяти. 15. Файл, папка, каталог. 16. Разграничение доступа к объектам операционной системы. 17. Комплексная система организации управления доступом. 18. Инсталляция. Настройка. 19. Аудит безопасности операционной системы. 20. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 21. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 22. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и	52

<table>
<tr><td></td><td colspan="2">распределенные МЭ.
23. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
24. Концепция построения виртуальных защищенных сетей;.
25. Виртуальные защищенные сети.
26. Туннелирование.
27. Инкапсуляция пакетов.
28. Структура защищенного пакета.
29. Варианты построения защищенных каналов.
30. Защита на канальном уровне.
31. ПротоколыPPTP, L2F, L2TP.
32. Протоколы формирования защищенных каналов на сеансовом уровне.
33. Протоколы SSL, TLS, SOCKS.
34. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.
35. Защита на прикладном уровне.
36. Протоколы PAP, CHAP, S/Key, SSO, Kerberos.
37.
38. Функционирование системы управления средствами защиты.
39. Аудит безопасности информационной системы.</td><td></td></tr>
<tr><td rowspan="14">Курсовой проект</td><td colspan="2">Обязательные аудиторные учебные занятия по курсовому проекту</td><td rowspan="14">30</td></tr>
<tr><td>1</td><td>Введение. Выдача заданий</td></tr>
<tr><td>2</td><td>Анализ поставленной задачи</td></tr>
<tr><td>3</td><td>Определение защищаемых информационных активов. Категорирование информации</td></tr>
<tr><td>4</td><td>Определение уязвимостей и угроз</td></tr>
<tr><td>5</td><td>Анализ и выбор возможных решений по защите</td></tr>
<tr><td>6</td><td>Анализ механизмов защиты</td></tr>
<tr><td>7</td><td>Анализ требуемых компонентов</td></tr>
<tr><td>8</td><td>Проектирование модели угроз</td></tr>
<tr><td>9</td><td>Настройка компонентов защиты</td></tr>
<tr><td>10</td><td>Конфигурирование пользовательских задач</td></tr>
<tr><td>11</td><td>Проектирование эксперимента по внедрению системы защиты</td></tr>
<tr><td>12</td><td>Нормативно-правовое обеспечение проекта</td></tr>
<tr><td>13</td><td>Расчет индекса ROSI</td></tr>
</table>

	14	Подготовка пояснительной записки к курсовому проекту	
	15	Защита курсового проекта	
Тематика курсовых проектов (работ):	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.		
Учебная практика МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**Виды работ:**		
	1	Работа с учетными записями пользователей	72
	2	Настройка параметров безопасности ОС	
	3	Управление хранением данных.	
	4	Архивация данных	
	5	Восстановление данных	
	6	Аудит ресурсов ОС	
	7	Аудит событий ОС	
	8	Управление доступом в Linux	
	9	Управление доступом в Windows	

	10	Средства аутентификации операционных систем	
	11	Управление средствами аутентификации в Linux	
	12	Управление средствами аутентификации в Windows	
	13	Документирование политики безопасности	
	14	Выбор, подключение, настройка межсетевого экрана	
	15	Выбор, подключение, настройка межсетевого экрана	
	16	Администрирование межсетевого экрана	
	17	Ознакомление, подключение, настройка системы резервного копирования	
	18	Ознакомление, подключение, настройка системы резервного копирования	
	19	Администрирование системы резервного копирования	
	20	Администрирование системы резервного копирования	
	21	Ознакомление, подключение, настройка системы антивирусной защиты	
	22	Администрирование системы антивирусной защиты.	
	23	Изучение методов комплексного исследования объекта информатизации	
	24	Изучение информации циркулирующей в корпоративной информационной системе	
	25	Изучение построения системы защиты информации на основе нормативных актов и методических указаний	
	26	Изучение построения системы защиты информации на основе нормативных актов и методических указаний	
	27	Построение модели угроз ИСПДн	
	28	Определение вероятности реализации угроз безопасности в информационной системе персональных данных	
	29	Изучение действующей нормативной документации объекта информатизации	
	30	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	31	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	32	Составление плана мероприятий по улучшению защищённости объекта информатизации	
	33	Разработка КСЗИ информационной системы: сбор данных	
	34	Разработка КСЗИ информационной системы: выбор технологий	

	35	Разработка КСЗИ информационной системы: разработка модели	
	36	Разработка КСЗИ информационной системы: оформление решения	
Промежуточная аттестация в форме дифференцированного зачета			**4**
Раздел 2.Криптографическая защита информации			**178**
МДК 02.02.Криптографическая защита информации			178
Тема 2.1. Основы криптографических методов защиты информации	**Содержание учебного материала**		**30**
	1	**Занятие 1. Введение в криптографию** Основные понятия и определения. Основные этапы развития криптографии. Становление криптографии как науки.	
	2	**Занятие 2. Задачи криптографии** Основные задачи криптографии. Управление секретными ключами. Инфраструктура открытых ключей. Модели открытых текстов. Вероятностная модель открытого текста. Критерии распознавания открытых текстов. Формальные модели шифров. Алгебраическая модель шифра. Вероятностная модель шифра	
	3	**Занятие 3. Свойства информационной безопасности.** Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности.	
	4	**Занятие 4. Криптографические методы.** Шифрование. Кодирование. Стеганография. Сжатие.	
	5	**Занятие 5. Математика криптографии.** Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение.	
	6	**Занятие 6. Классификация шифров.** Поточные шифры замены. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Дисковые шифраторы. Шифры гаммирования. Использование неравновероятностной гаммы. Повторное использование гаммы. Криптоанализ шифра Вижинера.	
	7	**Занятие 7. Классификация шифров** Шифры перестановки. Разновидности шифров перестановки. Элементы криптоанализа шифров перестановки.	
	8	**Занятие 8. Блочные шифры**.	

		Блочные шифры простой замены. Шифры Плейфера и Хилла. Архитектура современных блочных шифров: сеть Фейстеля. Режимы использования блочных шифров. Российский блочный шифр ГОСТ 28147-89. Криптоалгоритмы: RINJDAEL и IDEA. Методы анализа алгоритмов блочного шифрования. Рекомендации по практическому применению алгоритмов блочного шифрования.	
	9	**Занятие 9. Системы шифрования с открытым ключом.** Принцип ассиметричного шифрования. Практические аспекты использования криптосистем с открытым ключом.	
	10	**Занятие 10. Криптографическая стойкость шифров.** Теоретическая и практическая стойкость шифров. Подходы к определению криптографической стойкости шифров. Подходы к определению практической стойкости шифров. Имитостойкость шифров. Имитозащита. Характеристики имитостойкости шифров и их оценки.	
	11	**Занятие 11. Поточные шифры** Принципы построения алгоритмов поточного шифрования. Строение поточных криптосистем. Генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложности решения задач теории чисел. Генераторы на основе линейных регистров сдвига.	
	12	**Занятие 12. Методы анализа криптографических алгоритмов** Классификация методов анализа криптографических алгоритмов. Методы нахождения ключей криптографических алгоритмов: алгоритмические методы, алгебраические методы, статистические методы	
	13	**Занятие 13. Криптографические хеш-функции** Общие сведения о хеш-функциях. Криптографические хеш-функции. Ключевые и бесключевые хеш-функции. Итеративные способы построения хеш-функций. Понятие о стойкости хеш-функций.	
	14	**Занятие 14. Компьютерное шифрование.** Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	
	15	**Занятие 15. Криптоанализ.** Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста .	
	Практические занятия		
	1	**Занятие 16**. Стеганографические методы скрытия информации	**14**
	2	**Занятие 17**. Применение методов шифрования перестановкой	

	3	**Занятие 18**. Применение методов шифрования заменой	
	4	**Занятие 19**. Применение методов шифрования многоалфавитной замены	
	5	**Занятие 20**. Криптоанализ методов перестановки	
	6	**Занятие 21**. Криптоанализ методов замены	
	7	**Занятие 22**. Компьютерное шифрование	
Тема 2.2. Современные стандарты шифрования	**Содержание учебного материала**		**18**
	1	**Занятие 23. Принципы построения криптографических алгоритмов с симметричными ключами** Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Различие между программными и аппаратными реализациями. Программные реализации шифров. Современные криптографические интерфейсы.	
	2	**Занятие 24. Принципы построения криптографических алгоритмов с несимметричными ключами** Криптографические стандарты. Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применения дискретных функций для усложнения последовательностей.	
	3	**Занятие 25. Симметричное шифрование.** Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES.	
	4	**Занятие 26. Усовершенствованный стандарт шифрования AES**. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES.	
	5	**Занятие 27. Российские стандарты симметричного шифрования** Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015.	
	6	**Занятие 28. Проблема распределения ключей симметричного шифрования.** Алгоритм Диффи-Хелмана. Управление ключами. Kerberos.	
	7	**Занятие 29. Асимметричное шифрование** Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы.	

	8	**Занятие 30. Асимметричное шифрование** Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП.	
	9	**Занятие 31. Российские стандарты асимметричного шифрования.** ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	
	Практические занятия		
	6	**Занятие 32.** Алгоритм Диффи-Хелмана	**10**
	7	**Занятие 33. С**тандарт симметричного шифрования AES RIJNDAEL	
	8	**Занятие 34.** Генерация простых чисел, используемых в асимметричных системах шифрования	
	9	**Занятие 35.** Криптографические хэш-функции. Аутентификация.	
	10	**Занятие 36.** Шифрование методом скользящей перестановки	
	Лабораторные работы		
	1	**Занятие 37.** Изучение программных продуктов защиты информации. Программа PGP (Pretty Good Privacy)	**10**
	2	**Занятие 38.** Шифр Плейфера.	
	3	**Занятие 39.** Российский стандарт хэш-функции ГОСТ Р 34.11-94	
	4	**Занятие 40.** Криптосистема RSA	
	5	**Занятие 41.** Электронная цифровая подпись	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание учебного материала**		
	1	**Занятие 42. Целостность сообщения.** Случайная модель Orac1e. Установление подлинности сообщения.	
	2	**Занятие 43. 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.	
	3	**Занятие 44. Электронная цифровая подпись.** Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи.	**28**
	4	**Занятие 45. Электронная цифровая подпись.** Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012.	
	5	**Занятие 46. Установление подлинности объекта**. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым	

		разглашением	
	6	**Занятие 47. Технологии идентификации** Биометрические средства идентификации. Электронные ключи и карты. Токены.	
	7	**Занятие 48. Сертификаты открытого ключа** Проблемы распределения открытого ключа асимметричного шифрования. Удостоверяющие центры. X.509. Иерархия PKI.	
	8	**Занятие 49. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне.** Электронная почта. Архитектура e-mail. PGP. S/M1ME	
	9	**Занятие 50. Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне.** Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети	
	10	**Занятие 51. Защита информации в сетях беспроводного доступа.** IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16.	
	11	**Занятие 52. Защита информации в сетях сотовой связи.** A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи.	
	12	**Занятие 53. Прикладные программные интерфейсы, реализующие средства защиты информации** Защищенные транспортные протоколы. Программно-аппаратные средства защиты информации. Защищенный протокол HTTPS. Вопросы безопасности в Интернет протоколах.	
	13	**Занятие 54. Принципы работы технологии блокчейн** Реализация блокчейна Ethereum. Основные компоненты системы. Состояние учетной записи. Блоки экосистемы Ethereum. Хэш и сложность блока.	
	14	**Занятие 55. Принципы работы технологии блокчейн** Транзакции, сборы и «газ». Хэш транзакции. Принцип работы цифрового дерева Меркла. Фильтр Блума.	
	15	**Занятие 56. Принципы работы технологии блокчейн** Технический стандарт ERC20 для разработки смарт-контракта. Написание смарт-контракта на языке Solidity. Эмиссия цифровых токенов.	
	16	**Занятие 57. Блокчейн в системах искусственного интеллекта**	

		ICO как краудфандинговая платформа. Сопровождение ICO в России. Юрисдикционные вопросы в аспекте законодательства о криптовалютах, регуляция SEC. Оформление ICO через различные правовые конструкции.	
	17	**Занятие 58. Основы квантовой криптографии** Что такое квантовая криптография, и какие задачи она решает. Одноразовые ключи. Критерий Шеннона абсолютной секретности. Существующие достижения в квантовой криптографии.	
	18	**Занятие 59. Основы математического аппарата квантовой информатики.** Описание квантовых состояний отдельных и составных квантовых систем, чистые, смешанные состояния, квантовая запутанность, ортогональные и обобщенные измерения, очищение квантовых состояний, теорема о запрете копирования, преобразования квантовых систем, вполне положительные отображения.	
	19	**Занятие 60. Меры близости квантовых состояний, используемые в протоколах квантовой криптографии.** Теорема о невозможности копирования и протокол квантовой телепортации.	
	20	**Занятие 61. Протоколы квантового распределения ключей**. Основные протоколы квантового распределения ключей: BB84, B92, E91, SARG04, фазово-временное кодирование, дифференциально-фазовое кодирование.	
	21	**Занятие 62. Когерентные состояния и их преобразования оптическими элементами**.	
	22	**Занятие 63. Волоконные реализации систем квантовой криптографии**	
	23	**Занятие 64. Технологии защищенной обработки информации** Применение технологии терминального доступа. Общие сведения о технологии терминального доступа. Обеспечение безопасности сервера ОС Windows Server. Настройка сервера MSTS. Настройка протокола RDP.	
	24	**Занятие 65. Технологии защищенной обработки информации** Службы каталогов. Общие сведения о службах каталогов. Структура каталога LDAP. Система единого входа в сеть на основе протокола Kerberos. Создание единого пространства безопасности на базе Active Directory.	
	25	**Занятие 66. Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации** Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации (далее - система аттестации), как составной части единой системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Цели и виды аттестации объектов информатизации на	

		соответствие требованиям безопасности информации. Участники аттестации и их полномочия (компетенции). Задачи, функции, права и обязанности органов по аттестации	
	26	**Занятие 67. Требования к органам по аттестации объектов информатизации** Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации	
	27	**Занятие 68. Основные мероприятия по проведению аттестации объектов информатизации на соответствие требованиям безопасности информации** Подача и рассмотрение заявки на аттестацию объектов информатизации. Предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний. Проведение аттестационных испытаний объектов информатизации. Оформление, регистрация и выдача аттестата соответствия	
	28	**Занятие 69. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объекта информатизации.** Программа и методики аттестационных испытаний объектов информатизации. Аттестат соответствия	
	29	**Занятие 70. Сертификация объектов** Назначение и общая характеристика. Добровольная сертификация. Обязательное подтверждение соответствия. Декларирование соответствия. Обязательная сертификация	
	30	**Занятие 71. Сертификация объектов** Проведение сертификационных испытаний: принципы проведения испытаний, документы сертификационных испытаний. Сертификация продукции, ввозимой из-за границы РФ. Сертификация на региональном и международном уровнях.	
	31	**Занятие 72. Методики внедрения программно-аппаратных средств криптографической защиты** Пакет PGP, пакет Криптон	
	32	**Занятие 73. Методики внедрения программно-аппаратных средств криптографической защиты** СКЗИ «Верба-О», ПК «Inter-PRO»	
	Лабораторные работы		**10**
	6	**Занятие 74.** Разработка схемы простого пароля	

	7	**Занятие 75.** Разработка схемы динамического пароля	
	8	**Занятие 76.** Сертификаты открытого ключа	
	9	**Занятие 77.** Настройка и администрирование токена	
	10	**Занятие 78.** Настройка сервисов Рутокен	
	Самостоятельная работа обучающихся		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. **Тематика домашних заданий, сообщений, рефератов:** 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. 9. Поточные и блочные шифры. 10. Традиционные шифры замены. 11. Шифры многоалфавитной замены. Частотность символов. 12. Криптоанализ. 13. Атака грубой силы. 14. Частотный анализ. 15. Атака по образцу. 16. Атака знания исходного текста. 17. Компьютерное шифрование. 18. Стандарт шифрования данных DES. 19. Структура DES. Безопасность DES. 20. Структура ГОСТ 28147-89. 21. Режимы шифрования ГОСТ 28147 22. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 23. Алгоритм Диффи-Хелмана.	**18**

	24. Управление ключами. Kerberos. 25. Асимметричное шифрование. 26. Криптографическая система Эль-Гамаля. 27. ГОСТ 34.10-94. 28. ГОСТ Р 34.10-2001. 29. ГОСТ Р 34.10 -2012. **Тематика научных работ обучающихся:** 1. Типы атак. Атаки, в основе которых лежит парадокс задачи о днях рождения. Двусторонние атаки. Уровень безопасности. Освоение процессов зашифрования и расшифрования для простейших шифров 2. Частотные свойства осмысленных сообщений. 3. Криптоанализ шифра однобуквенной простой замены 4. Криптоанализ шифра «решетка Кардано». 5. Вскрытие шифра Вернама при повторном использовании ключа. Криптоанализ шифра Виженера. 6. Шифры, основанные на алгоритме Фейстеля. Функция раунда. Реализация функции раунда. Традиционные симметричные блочные шифры. 7. Расчет метода встречных атак. 8. Канальное и сквозное шифрование. Управление секретными ключами. Криптоанализ рассмотренных алгоритмов симметричного шифрования. Размер ключа. 9. Цифровые подписи. Управление ключами. Взлом ключа. Согласование ключей с помощью пароля. Защищенные функции хэширования. HMAC. SHA. MD5. RIPEMD. UMAC. Криптография с открытым ключом. 10. Обмен ключами. Схема Диффи-Хеллмана. Протокол обмена ключами Oakley, ISAKMP 11. Серверы ключей. Система Kerberos. Сервис аутентификации X.509. 12. Стохастическое преобразование информации. R-блоки. Гаммирование. Вероятностное шифрование. 13. Изучение системы PGP 14. Пример реализации защиты информации на предприятии (представить свой вариант ПО позволяющего защитить секретные данные от несанкционированного копирования, в качестве варианта использовать пред-приятие, работающее на 1С, не исключать использование копирования информации на электронные носители и выход в Интернет). 15. Брандмауэры.	

	16. Троянские кони. Принцип действия. Защита 17. Черви. Принцип действия. Защита 18. Криптосистемы с открытым ключом (ассиметричные) 19. Свойства конструкции безусловно стойких шифров, названных К. Шенноном совершенными, по отношению к различным криптоатакам. 20. Квантовая криптография. 21. Цифровая подпись. Реализация. Плюсы и минусы ее использования. 22. Вероятностное шифрование. 23. Криптографическое сжатие. Алгоритмы сжатия данных. Арифметическое кодирование. 24. Беспроводные сети. Атаки. Механизмы обеспечения защиты информации. Протокол WEP. 25. Последние разработки в криптографии (разбор современнейших подходов к шифрованию, исключая квантовое) 26. Модель обработки сообщений и защиты пользователя. Управление доступом на основе представлений. 27. Режим сцепления шифрованных блоков. Электронная шифровальная книга.	
Промежуточная аттестация в форме дифференцированного зачета		**4**
Учебная практика МДК.02.02. Криптографическая защита информации	**Виды работ**	36
	1 Настройка и администрирование токена	
	2 Настройка сервисов Рутокен-PinPad	
	3 Настройка сервисов Рутокен-ЭЦП	
	4 Настройка сервисов Рутокен–Bluetooth	
	5 Настройка сервисов Рутокен–S	
	6 Разработка алгоритма PGP	
	7 Изучение протоколов SSL, TLS, IPSec	
	8 Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	
	9 Составление алгоритма хеш-функции	
	10 Составление алгоритма шифра	
	11 Подключение, установка драйверов, настройка программных средств шифрования Криптон.	
	12 Администрирование программных средств шифрования Криптон	

	13	Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон.	
	14	Администрирование аппаратных средств шифрования Криптон.	
	15	Инфраструктуры открытых ключей и стандарт X.509	
	16	Защита электронного документооборота с использованием электронной цифровой подписи	
	17	Программная реализация ГОСТ Р 34.12- 2015	
	18	Стандарты информационной безопасности в Интернете (IETF, RFC).	
Производственная практика (по профилю специальности)	**Виды работ**		180
	1	Инструктаж по технике безопасности	
	2	Ознакомление с рабочим местом	
	3	Ознакомление с организационной структурой предприятия	
	4	Резервное копирование информации	
	5	Восстановление данных	
	6	Проверка копий на предприятии, изучение технологии резервного копирования	
	7	Защита информации от несанкционированного доступа	
	8	Защита информации от несанкционированного доступа	
	9	Защита информации от несанкционированного доступа	
	10	Регистрация и учёт входа/выхода субъектов системы в/из системы (узла сети)	
	11	Регистрация и учёт входа/выхода субъектов системы в/из системы (узла сети)	
	12	Учёт носителей информации	
	13	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	
	14	Работа с антивирусами	
	15	Работа с антивирусами	
	16	Обновление антивирусных программ	
	17	Защита почтовых ящиков	
	18	Шифрование конфиденциальной информаци	
	19	Работа в программе cryptoapi	
	20	Работа в программе cryptoapi	
	21	Работа в программе cryptoapi	
	22	Работа в программе Windows Defender	
	23	Работа в программе Windows Defender	

	24	Работа в программе Windows Defender	
	25	Изучение дискреционного принципа контроля доступа к информации	
	26	Изучение дискреционного принципа контроля доступа к информации	
	27	Создание системы защиты персональных данных	
	28	Создание системы защиты персональных данных	
	29	Создание системы защиты персональных данных	
	30	Создание системы защиты персональных данных	
	31	Создание системы защиты персональных данных	
	32	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	33	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	34	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	35	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	36	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	37	Создание комплекса мероприятий по защите персональных данных с использованием резервного копирования, шифрования информации, антивирусных программ	
	38	Участие в организации работ по защите персональных компьютеров на предприятии	
	39	Участие в организации работ по защите персональных компьютеров на предприятии	
	40	Участие в организации работ по защите персональных компьютеров на предприятии	
	41	Участие в организации работ по защите персональных компьютеров на предприятии	
	42	Участие в организации работ по защите локальных сетей на предприятии	
	43	Участие в организации работ по защите локальных сетей на предприятии	
	44	Участие в организации работ по защите локальных сетей на предприятии	
	45	Участие в организации работ по защите работ в глобальной сети интернет на предприятии	
	46	Участие в организации работ по защите работ в глобальной сети интернет на предприятии	
	47	Участие в организации работ по защите работ в глобальной сети интернет на предприятии	
	48	Работа с криптографическими средствами защиты информации	
	49	Работа с криптографическими средствами защиты информации	

	50	Работа с криптографическими средствами защиты информации	
	51	Работа с криптографическими средствами защиты информации	
	52	Работа с криптографическими средствами защиты информации	
	53	Работа с криптографическими средствами защиты информации	
	54	Работа с криптографическими средствами защиты информации	
	55	Работа с криптографическими средствами защиты информации	
	56	Работа с криптографическими средствами защиты информации	
	57	Работа с криптографическими средствами защиты информации	
	58	Работа с криптографическими средствами защиты информации	
	59	Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.	
	60	Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.	
	61	Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети.	
	62	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	63	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	64	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	65	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	66	Администрирование систем безопасности беспроводной защищенной локальной сети.	
	67	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	
	68	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	
	69	Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей.	
	70	Выбор программных средств шифрования в соответствии с решаемой задачей	
	71	Выбор программных средств шифрования в соответствии с решаемой задачей	
	72	Выбор программных средств шифрования в соответствии с решаемой задачей	

	73	Подключение, установка драйверов, настройка программных средств абонентского шифрования	
	74	Подключение, установка драйверов, настройка программных средств абонентского шифрования	
	75	Подключение, установка драйверов, настройка программных средств абонентского шифрования	
	76	Администрирование внедренных средств	
	77	Администрирование внедренных средств	
	78	Администрирование внедренных средств	
	79	Настройка средств электронной подписи	
	80	Настройка средств электронной подписи	
	81	Настройка средств электронной подписи	
	82	Администрирование средств электронной подписи	
	83	Администрирование средств электронной подписи	
	84	Администрирование средств электронной подписи	
	85	Администрирование средств PKI	
	86	Администрирование средств PKI	
	87	Администрирование средств PKI	
	88	Сдача рабочего места	
	89	Подготовка дневника и аттестационного листа по практике	
	90	Подготовка и сдача отчета по практике	
Самостоятельная работа при подготовке к экзамену по профессиональному модулю			**8**
Консультации			**2**
Промежуточная аттестация в форме экзамена по профессиональному модулю			**8**
Всего по ПМ			**776**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы предусмотрены следующие специальные помещения:

Лаборатория «Программных и программно-аппаратных средств защиты информации». Лаборатория оснащена антивирусными программными комплексами; аппаратными средствами аутентификации пользователя; программно-аппаратными средствами управления доступом к данным и защиты (шифрования) информации; средствами защиты информации от НСД, блокирования доступа и нарушения целостности; программными средствами криптографической защиты информации; программными средствами 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; комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2 Информационное обеспечение реализации программы

3.2.1. Нормативные документы:

1. Кодекс Российской Федерации об административных правонарушениях//Гарант: справочно-правовая система. – URL: https://base.garant.ru/12125267/ (дата обращения: 22.02.2023).
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12148555/ (дата обращения: 22.02.2023).
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12148567/(дата обращения: 22.02.2023).
4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12129354/(дата обращения: 22.02.2023).
5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12185475/(дата обращения: 22.02.2023).
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/12136635/(дата обращения: 22.02.2023).
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/10200083/(дата обращения: 22.02.2023).
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» //Гарант: справочно-правовая система. – URL: https://base.garant.ru/192944/(дата обращения: 22.02.2023).
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608//Гарант: справочно-правовая система. – URL: https://base.garant.ru/102670/(дата обращения: 22.02.2023).
10. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г. //Федеральная

служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/en/component/attachments/download/288(дата обращения: 22.02.2023).
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21 //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21(дата обращения: 22.02.2023).
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. //Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument(дата обращения: 22.02.2023).
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 17 июля 2017 г. N 134// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/1362-prikaz-fstek-rossii-ot-17-iyulya-2017-g-n-134-2(дата обращения: 22.02.2023).
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/administrativnye-reglamenty/478-prikaz-fstek-rossii-ot-12-iyulya-2012-g-n-84(дата обращения: 22.02.2023).
15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702(дата обращения: 22.02.2023).
16. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/370 (дата обращения: 22.02.2023).
17. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». – URL: https://base.garant.ru/187947/(дата обращения: 22.02.2023).
18. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200095034(дата обращения: 22.02.2023).
19. ГОСТ Р 34-11-2012. Информационная технология. Криптографическая защита информации. Функция хэширования//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200095035(дата обращения: 22.02.2023).

20. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. –URL: http://docs.cntd.ru/document/1200058320(дата обращения: 22.02.2023).
21. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/gost-r-51275-2006 (дата обращения: 22.02.2023).
22. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 22.02.2023).
23. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. – URL: http://docs.cntd.ru/document/1200102287(дата обращения: 22.02.2023).
24. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200044725 (дата обращения: 22.02.2023).
25. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200113006(дата обращения: 22.02.2023).
26. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200113336(дата обращения: 22.02.2023).
27. 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//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200048398(дата обращения: 22.02.2023).
28. 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//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс». – URL: https://docs.cntd.ru/document/1200101777(дата обращения: 22.02.2023).
29. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200105710(дата обращения: 22.02.2023).
30. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: https://docs.cntd.ru/document/1200105711(дата обращения: 22.02.2023).

31. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. - URL: http://docs.cntd.ru/document/1200103619(дата обращения: 22.02.2023).
32. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010(дата обращения: 22.02.2023).
33. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети//Электронный фонд правовых и нормативно-технических документов/Консорциум «Кодекс»: официальный сайт. – URL: http://docs.cntd.ru/document/1200048416(дата обращения: 22.02.2023).
34. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.// Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380(дата обращения: 22.02.2023).

3.2.2. Основные электронные издания:

1. Потерпеев, Г. Ю. Безопасность операционных систем: учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва: РТУ МИРЭА, 2021. — 93 с. —ISBN 978-5-7339-1393-3. — URL: https://e.lanbook.com/book/182416 (дата обращения: 22.02.2023).
2. Староверова, Н. А. Операционные системы: учебник / Н. А. Староверова. — Санкт-Петербург: Лань, 2022. — 308 с. — ISBN 978-5-8114-4000-9. — URL: https://e.lanbook.com/book/207089(дата обращения: 22.02.2023).
3. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с. — ISBN 978-5-7883-1526-3. — URL: https://e.lanbook.com/book/189043(дата обращения: 22.02.2023).
4. Иванюгин, В. М. Администрирование безопасности ОС Windows инструментальными средствами: методические указания / В. М. Иванюгин. — Москва: РТУ МИРЭА, 2020. — 104 с. — URL: https://e.lanbook.com/book/163832(дата обращения: 22.02.2023).
5. Мошак, Н. Н. Защищенные информационные системы: учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. — URL: https://e.lanbook.com/book/180099(дата обращения: 22.02.2023).
6. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — URL: https://e.lanbook.com/book/237770 (дата обращения: 22.02.2023).
7. Сергеев, А. Н. Основы локальных компьютерных сетей: учебное пособие для вузов / А. Н. Сергеев. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 184 с. — ISBN 978-5-507-44766-4. — URL: https://e.lanbook.com/book/242867(дата обращения: 22.02.2023).

8. Бутакова, Н. Г. Криптографические методы и средства защиты информации: учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург: Интермедия, — ISBN 978-5-4383-0210-0. - URL: https://ibooks.ru/products/374947(дата обращения: 22.02.2023).
9. Введение в криптографическую защиту информации объектов: учебник / С. Н. Ильиных, С. Г. Алюшина, Т. И. Калинкина [и др.]. — Москва: МТУСИ, 2021. — — URL: https://e.lanbook.com/book/215231 (дата обращения: 22.02.2023).
10. Прохорова, О. В. Информационная безопасность и защита информации: учебник для вузов / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2021. — 124 с. — — ISBN 978-5-8114-7970-2. — URL: https://e.lanbook.com/book/169817(дата обращения: 22.02.2023).
11. Нестеров, С. А. Основы информационной безопасности: учебник для вузов / С. А. Нестеров. — Санкт-Петербург: Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — URL: https://e.lanbook.com/book/165837(дата обращения: 22.02.2023).
12. Епишкина, А. В. Нормативное регулирование в области защиты информации: Конспект лекций: учебное пособие / А. В. Епишкина, С. В. Запечников. — Москва: — ISBN 978-5-7262-2807-5. —URL: https://e.lanbook.com/book/284345. (дата обращения: 22.02.2023).
13. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение: учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 392 с. — ISBN 978-5-8114-8514-7. — URL: https://e.lanbook.com/book/176657. (дата обращения: 22.02.2023).
14. Поляков, Е. А. Основы информационной безопасности: учебное пособие / Е. А. — URL: https://e.lanbook.com/book/282890. (дата обращения: 22.02.2023).
15. Шелухин, О. И. Учебно-методическое пособие по дисциплине «Интеллектуальные технологии информационной безопасности анонимизация и деанонимизация пользователей Интернет-порталов»: учебно-методическое пособие / О. И. Шелухин, А. В. Ванюшина; составители О. И. Шелухин, А. В. Ванюшина. — Москва: МТУСИ, 2021. — 49 с. — URL: https://e.lanbook.com/book/215345. (дата обращения: 22.02.2023).
16. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — URL: https://e.lanbook.com/book/156401. (дата обращения: 22.02.2023).
17. Гладких, А. А. Основы современных криптографических систем и перспективы их развития: учебное пособие / А. А. Гладких, В. Е. Дементьев, Н. Ю. Чилихин. — Ульяновск: УлГТУ, 2020. — 214 с. — ISBN 978-5-9795-2096-4. — URL: https://e.lanbook.com/book/259745. (дата обращения: 22.02.2023).
18. Васин, Н. Н. Моделирование виртуальных частных сетей VPN: методические указания / Н. Н. Васин, Е. М. Аленников, А. Ю. Субботская. — Самара: ПГУТИ, 2020. — 30 с. — URL: https://e.lanbook.com/book/255623. (дата обращения: 22.02.2023).
19. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем: учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва: РТУ МИРЭА, 2020. — 136 с. — URL: https://e.lanbook.com/book/167606. (дата обращения: 22.02.2023).
20. Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия: учебное пособие / В. М. Бабушкин. — — ISBN 978-5-7579-2463-2. — URL: https://e.lanbook.com/book/193486. (дата обращения: 22.02.2023).
21. Страшун, Ю. П. Технические средства автоматизации и управления на основе IIoT/IoT: учебное пособие / Ю. П. Страшун. — Санкт-Петербург: Лань, 2020. — 76

с. — ISBN 978-5-8114-5018-3. — URL: https://e.lanbook.com/book/143701(дата обращения: 22.02.2023).
22. Лагоша, О. Н. Сертификация информационных систем: учебное пособие / О. Н. Лагоша. — Санкт-Петербург: Лань, 2020. — 112 с. — ISBN 978-5-8114-4668-1. — URL: https://e.lanbook.com/book/139268 (дата обращения: 22.02.2023).
23. Введение в теоретико-числовые методы криптографии: учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург: Лань, 2022. — 400 с. — ISBN 978-5-8114-1116-0. — URL: https://e.lanbook.com/book/210746 (дата обращения: 22.02.2023).
24. Игнатьев, Е. Б. Основы криптографии: учебное пособие / Е. Б. Игнатьев. — Иваново: ИГЭУ, 2020. — 88 с. — URL: https://e.lanbook.com/book/154559 (дата обращения: 22.02.2023).
25. Леонтьев, А. С. Защита информации: учебное пособие / А. С. Леонтьев. — Москва: РТУ МИРЭА, 2021. — 79 с. — URL: https://e.lanbook.com/book/182491 (дата обращения: 22.02.2023).
26. Каширская, Е. Н. Криптографический анализ и методы защиты информации: учебное пособие / Е. Н. Каширская. — Москва: РТУ МИРЭА, 2020. — 91 с. — URL: https://e.lanbook.com/book/163861(дата обращения: 22.02.2023).
27. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — — ISBN 978-5-8114-4042-9. — URL: https://e.lanbook.com/book/206285 (дата обращения: 22.02.2023).
28. Сковиков, А. Г. Цифровая экономика. Электронный бизнес и электронная коммерция: учебное пособие для вузов / А. Г. Сковиков. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 260 с. — ISBN 978-5-8114-6857-7. — URL: https://e.lanbook.com/book/152653(дата обращения: 22.02.2023).
29. Цареградская, Ю. К. Правовое регулирование и юридическое сопровождение ICO: учебное пособие / Ю. К. Цареградская. — Москва: Проспект, 2021. — 768 с.— ISBN 978-5-392-33764-4. - URL: https://ibooks.ru/products/380187 (дата обращения: 22.02.2023).
30. Прилипко, В. К. Физические основы квантовых вычислений. Динамика кубита: монография / В. К. Прилипко, И. И. Коваленко. — Санкт-Петербург: Лань, 2022. — 216 с. — ISBN 978-5-8114-3383-4. — URL: https://e.lanbook.com/book/205985 (дата обращения: 22.02.2023).
31. Граймс, Р. А. Апокалипсис криптографии: подготовка к квантовому прорыву: практическое руководство / Р. Граймс; пер. с англ. В. А. Яроцкого. - Москва: ДМК Пресс, 2020. - 290 с. — ISBN 978-5-93700-050-7. - URL: https://ibooks.ru/products/388436 (дата обращения: 22.02.2023).
32. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — URL: https://e.lanbook.com/book/207095 (дата обращения: 22.02.2023).

Электронные ресурсы:

35. Федеральная служба по техническому и экспортному контролю (ФСТЭК России): официальный сайт. - URL: www.fstec.ru. (дата обращения: 22.02.2023).
36. Elibrary.ru. Научная электронная библиотека: официальный сайт. – URL: www.elibrary.ru. (дата обращения: 22.02.2023).
37. Глобус –Телеком: официальный сайт. – URL: http:/www.globus-telecom.com. (дата обращения: 22.02.2023).

38. Морион. Российский разработчик и производитель оборудования связи: официальный сайт. – URL: http://www.morion.ru/. (дата обращения: 22.02.2023).
39. Безопасность информационных технологий: рецензируемый научный журнал НИЯУ МИФИ: официальный сайт. - URL: http://bit.mephi.ru/. (дата обращения: 22.02.2023).
40. Вопросы кибербезопасности: научный, периодический, информационно-методический журнал: официальный сайт. - URL: http://cyberrus.com/ (дата обращения: 22.02.2023).
41. НАТЕКС: официальный сайт. – URL: http://www.nateks.ru/. (дата обращения: 22.02.2023).
42. ISKRATEL: официальный сайт. – URL: http://www.iskratel.com/. (дата обращения: 22.02.2023).
43. Промсвязь: официальный сайт. – URL: http://www.ps-ufa.ru/. (дата обращения: 22.02.2023).
44. 3M. Наука, воплощенная в жизнь: [сайт]. – URL: http://3m.com/ (дата обращения: 22.02.2023).
45. ОАО «Ферроприбор»: [сайт]. – URL: http://www.rusgates.ru/index/php (дата обращения: 22.02.2023).
46. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "PositiveTechnologies". – URL: http://www.securitylab.ru (дата обращения: 22.02.2023).

3.2.3. Дополнительные источники:

1. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/document?pid=1001363(дата обращения: 22.02.2023).
2. Зайцев, Е. И. Операционные системы: учебное пособие / Е. И. Зайцев, Р. Ф. — URL: https://e.lanbook.com/book/226634(дата обращения: 22.02.2023).
3. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019. - URL: https://znanium.com/catalog/product/1018901(дата обращения: 22.02.2023).
4. Иванюгин, В. М. Основы информационной безопасности. Алгоритмы шифрования данных: методические указания / В. М. Иванюгин. — Москва: РТУ МИРЭА, 2021. — 30 с. — URL: https://e.lanbook.com/book/182518(дата обращения: 22.02.2023).
5. Игнатьев, Е. Б. Основы криптографии: учебное пособие / Е. Б. Игнатьев. — Иваново: ИГЭУ, 2020. — 88 с. — URL: https://e.lanbook.com/book/154559(дата обращения: 22.02.2023).
6. Информационный мир XXI века. Криптография - основа информационной безопасности: методическое руководство / под ред. Э. А. Болелова; Московский государственный технический университет гражданской авиации. - 4-е изд. — Москва: Дашков и К°, 2020. - URL: https://znanium.com/catalog/product/1081675(дата обращения: 22.02.2023).
7. Каширская, Е. Н. Криптографические системы: учебное пособие / Е. Н. Каширская, — URL: https://e.lanbook.com/book/182424(дата обращения: 22.02.2023).
8. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ: учебное пособие / А. Г. Киренберг. — Кемерово: КузГТУ имени Т.Ф. Горбачева, 2022. — 120 с. — URL: https://e.lanbook.com/book/257564(дата обращения: 22.02.2023).
9. Романьков, В.А. Введение в криптографию: курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. — Москва: Форум: ИНФРА-М, 2020. - URL: https://znanium.com/catalog/product/1046925(дата обращения: 22.02.2023).
10. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. – Москва: Горячая линия–Телеком, 2017. - URL: https://ibooks.ru/products/334031(дата обращения: 22.02.2023).

11. Семыкина, Н. А. Методы теории оптимального управления в задачах защиты компьютерных систем от вирусных атак: учебное пособие / Н. А. Семыкина. — Тверь: ТвГУ, 2020. — 100 с. — URL: https://e.lanbook.com/book/217949(дата обращения: 22.02.2023).
12. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов/О.И.Шелухин, Д.Ж.Сакалема, А.С.Филинова. - Москва: Горячая линия-Телеком, 2018. - URL: https://ibooks.ru/products/334051(дата обращения: 22.02.2023).

Периодические издания:

1. Защита информации Inside (дата обращения: 22.02.2023).
2. Проблемы информационной безопасности. Компьютерные системы. (дата обращения: 22.02.2023).
3. Information Security/Информационная безопасность: официальный сайт. - URL: https://lib.itsec.ru/imag/(дата обращения: 22.02.2023).

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; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации	Экспертное наблюдение

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-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
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 информации;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
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 Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
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 Экзамен
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 Экзамен
ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28		

Приложение 1

Информационные ресурсы, используемые при выполнении самостоятельной работы

*рекомендуется пользоваться Интернет-ресурсами при самостоятельной работе по всем разделам дисциплины

МДК 02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты

№ занятия	**Рекомендуемые учебные издания**
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	
Занятие1	[1] с. 7-12
Занятие 2	[1] с. 13-15
Занятие 3	[2] с. 286-289
Занятие 4	[3] с. 71-84
Занятие 5	[1] с. 68-77
Занятие 6	[4] с. 4-7
Занятие 7	[1] с. 68-77
Занятие 8	[3] с. 71-84
Занятие 9	[5] с.102-105
Занятие 10	[1] с.50-54
Занятие 11	[6] с. 50-77
Занятие 12	[1] с. 54-57, 75-80
Занятие 13	[2] с. 286-289
Занятие 14	[2] с. 289-295
Занятие 15	[3] с. 121-126
Занятие 16	[1] с. 49-56
Занятие 17	[1] с. 88-89
Занятие 18	[7] с. 109-114
Занятие 19	[5] с.102-105
Занятие 20	[1] с. 68-77
Занятие 21	[8] с. 300-303
Занятие 22	[8] с. 283-285
Занятие 23	[9] с. 246-264
Занятие 24	[10] с. 17-22
Занятие 25	[3] с. 12-14
Занятие 26	[3] с. 12-14
Занятие 27	[10] с. 18-19
Занятие 28	[11] с. 20-23
Занятие 29	[10] с. 19-22
Занятие 30	[10] с. 17-18
Занятие 31	[11] с. 30-32
Занятие 32	[12] с. 30-33
Занятие 33	[12] с. 42-45
Занятие 34	[12] с. 42-45
Занятие 35	[3] с. 19-20

Занятие 36	[3] с. 112-115
Занятие 37	[3] с. 112-115
Занятие 38	[1] с. 68-77
Занятие 39	[11] с. 117-121
Занятие 40	[5] с. 79-83
Занятие 41	[6] с. 143-151
Занятие 42	[6] с. 155-161
Занятие 43	[7] с. 123-124
Занятие 44	[8] с. 283-285
Занятие 45	[13] с. 29-31
Занятие 46	[5] с. 111-112
Занятие 47	[11] с. 117-121
Занятие 48	[14] с. 42-51
Занятие 49	[13] с. 352-357
Занятие 50	[15] с. 15-19
Занятие 51	[15] с. 15-19
Занятие 52	[9] с. 208-212
Занятие 53	[16] с. 187-190
Занятие 54	[11] с. 85-93
Занятие 55	[11] с. 85-93
Занятие 56	[13] с. 269-284
Занятие 57	[13] с. 269-284
Занятие 58	[3] с. 127-131
Занятие 59	[9] с. 259-264
Занятие 60	[9] с. 252-253
Занятие 61	[17] с. 108-110
Занятие 62	[3] с. 133-136
Занятие 63	[3] с. 127-131
Занятие 64	[3] с. 147-148
Занятие 65	[11] с. 85-93
Занятие 66	[11] с. 85-93
Занятие 67	[11] с. 112-116
Занятие 68	[18] с. 3-5, 11-12
Занятие 69	[18] с. 3-5, 11-12
Занятие 70	[18] с. 3-5, 11-12
Занятие 71	[16] с. 187-190
Занятие 72	[17] с. 164-170
Занятие 73	[17] с. 164-170
Занятие 74	[6] с. 149-150
Занятие 75	[19] с. 100-103
Занятие 76	[19] с. 100-103
Занятие 77	[20] с. 129-131
Занятие 78	[20] с. 172-174
Занятие 79	[20] с. 129-131

Занятие 80	[20] с. 131-133
Занятие 81	[20] с. 67-69
Занятие 82	[20] с. 67-69
Занятие 83	[21] с. 55-56
Занятие 84	[21] с. 55-56
Занятие 85	[20] с. 104-106
Занятие 86	[6] с. 166-168
Занятие 87	[3] с. 12-14
Занятие 88	[9] с. 252-253
Занятие 89	[6] с. 149-150
Занятие 90	[20] с. 129-131
Занятие 91	[19] с. 100-103
Занятие 92	[6] с. 149-150
Занятие 93	[11] с. 148-150
Занятие 94	[11] с. 148-150
Занятие 95	[20] с. 104-106
Занятие 96	[22] с. 63-65
Занятие 97	[22] с. 65-68
Занятие 98	[20] с. 67-69
Занятие 99	[11] с. 112-116
Занятие 100	[6] с. 166-168
Занятие 101	[20] с. 47-56
Занятие 102	[20] с. 47-56
Занятие 103	[11] с. 250-254

МДК.02.02.Криптографическая защита информации

№ занятия	**Рекомендуемые учебные издания**
Раздел 2.Криптографическая защита информации	
Занятие 1	[23] с. 5-9
Занятие 2	[9] с. 272
Занятие 3	[9] с. 269-272
Занятие 4	[24] с. 4-12
Занятие 5	[24] с. 24-25
Занятие 6	[24] с. 8-12
Занятие 7	[24] с. 8-12
Занятие 8	[24] с. 8-12
Занятие 9	[25] с. 14-16
Занятие 10	[25] с. 23-25
Занятие 11	[23] с. 5-9
Занятие 12	[26] с. 56-60
Занятие 13	[26] с. 56-60
Занятие 14	[9] с. 143-146
Занятие 15	[9] с. 246-247

Занятие 16	[9] с. 125-129
Занятие 17	[24] с. 24-25
Занятие 18	[9] с. 43-45
Занятие 19	[9] с. 50-55
Занятие 20	[9] с. 50-55
Занятие 21	[9] с. 84-92
Занятие 22	[9] с. 246-247
Занятие 23	[9] с. 20-21
Занятие 24	[9] с. 20-21
Занятие 25	[9] с. 20-21
Занятие 26	[9] с. 88-92
Занятие 27	[9] с. 118-120
Занятие 28	[9] с. 95-97
Занятие 29	[9] с. 107-109
Занятие 30	[9] с. 109-112
Занятие 31	[9] с. 140-143
Занятие 32	[9] с. 95-97
Занятие 33	[9] с. 88-92
Занятие 34	[9] с. 20-22
Занятие 35	[9] с. 20-22
Занятие 36	[9] с. 131-151
Занятие 37	[9] с. 46-50
Занятие 38	[27] с. 40-41
Занятие 39	[25] с. 66-67
Занятие 40	[9] с. 140-141
Занятие 41	[9] с. 155-157
Занятие 42	[9] с. 131-173
Занятие 43	[16] с. 180-181
Занятие 44	[9] с. 131-173
Занятие 45	[9] с. 131-173
Занятие 46	[9] с. 131-173
Занятие 47	[6] с. 51-53
Занятие 48	[11] с. 85-93
Занятие 49	[27] с. 40-41
Занятие 50	[11] с. 96-100
Занятие 51	[9] с. 236-238
Занятие 52	[9] с. 238-242
Занятие 53	[9] с. 249-251
Занятие 54	[28] с. 247-250
Занятие 55	[28] с. 247-251
Занятие 56	[28]
Занятие 57	[29] с.257-261
Занятие 58	[9] с. 272
Занятие 59	[29] с.250-254

Занятие 60	[30] с. 68-69
Занятие 61	[31] с.158-167
Занятие 62	[30] с. 68-69
Занятие 63	[30] с. 68-69
Занятие 64	[7] с. 135-137
Занятие 65	[7] с. 140
Занятие 66	[32] с.100-103
Занятие 67	[32] с.100-103
Занятие 68	[32] с.103-106
Занятие 69	[32] с.98-100
Занятие 70	[32] с.98-100
Занятие 71	[32] с.98-100
Занятие 72	[27] с. 40-41
Занятие 73	[27] с. 40-41
Занятие 74	[9] с. 246-248
Занятие 75	[9] с. 246-248
Занятие 76	[16] с. 187-190
Занятие 77	[9] с. 260-265
Занятие 78	[9] с. 260-265