

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Липецкий филиал Финуниверситета

СОГЛАСОВАНО


ПАО «Ростелеком»

Директор Липецкого филиала
ПАО «Ростелеком»


_____ К.В. Власов

УТВЕРЖДАЮ

Заместитель директора
по учебно-методической работе
Липецкого филиала Финуниверситета


_____ О.Н. Левчegov

«29» августа 2024 г.

«29» августа 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в информационно-телекоммуникационных
системах и сетях с использованием программных и программно-
аппаратных (в том числе, криптографических) средств защиты
по специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Липецк - 2024

Рабочая программа профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Черпаков Игорь Владимирович, к.ф.-м.н., доцент кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 27.08.2024 г. №1

Заведующий кафедрой

Учет и информационные технологии в бизнесе  Н.С. Морозова

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ.....	18
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ.....	25

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Рабочая программа профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» является частью основной профессиональной программы (далее ОПОП) в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа профессионального модуля «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке обучающихся данной специальности.

Рабочая программа составлена для обучающихся очной формы обучения, в том числе с применением элементов дистанционных образовательных технологий и электронного обучения.

При обучении инвалидов и лиц с ограниченными возможностями здоровья дистанционные образовательные технологии и электронное обучение предусматривает возможность приема-передачи информации в доступных для них формах.

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности организовывать ремонтные, монтажные и наладочные работы по промышленному оборудованию и соответствующие ему профессиональные компетенции:

ВД.2. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированных действий 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.

1.1.1. Перечень общих компетенций

ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.2. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	<ul style="list-style-type: none">– определения необходимых средств криптографической защиты информации;– использования программно-аппаратных криптографических средств защиты информации;– установки, настройки специализированного оборудования криптографической защиты информации;– применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; шифрования информации.
Уметь	<ul style="list-style-type: none">– выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах;– определять рациональные методы и средства защиты на объектах и оценивать их эффективность;– производить установку и настройку типовых программно-аппаратных средств защиты информации;– пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
Знать	<ul style="list-style-type: none">– типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах;– основные протоколы идентификации и аутентификации в телекоммуникационных системах;– состав и возможности типовых конфигураций программно-аппаратных средств защиты информации;– особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; основные способы противодействия– несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы;– основные понятия криптографии и типовые криптографические методы защиты информации;

1.2. Количество часов на освоение рабочей программы профессионального модуля

Всего часов: **546 час.**

Из них на освоение МДК – **346 час.:**

МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты – **244 час.;**

МДК.02.02 Криптографическая защита информации – **102 час.;**

В том числе самостоятельная работа – **148 час.**

Практики, в том числе учебная – **36 час.**

производственная (по профилю специальности) – **144 час.**

Курсовой проект (работа) в составе МДК – **20 час.**

Экзамен по модулю – **20 час.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональн ых и общих компетенций	Наименование разделов профессионального модуля (МДК)	Суммар ный объем нагрузк и, часов	В т.ч. в форме практической подготовки	Объем профессионального модуля, часов						
				Работа обучающихся во взаимодействии с преподавателем						Самосто ятельная работа
				Обучение по МДК				Практики		
				Всего	Промежу точная аттестац ия	В том числе		Учебна я	Произв одствен ная	
лаборато рные и практиче ские занятия	Курсовы е проекты (работы)									
ПК 2.1-2.3 ОК1-4, ОК 09	МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	244	-	134	10	54	20	-	-	100
ПК 2.1-2.3 ОК1-4, ОК 09	МДК. 02.02. Криптографическая защита информации	102	-	54	-	34	-	-	-	48
Учебная практика		36	36					36		
Производственная практика (по профилю специальности)		144	144						144	
Экзамен по модулю		20	X							
Всего:		546		188	10	88	20	36	144	148

2.2 Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля, междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) работа обучающихся	Объем часов
1	2	3
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		244
Тема 1.1. Обеспечение безопасности операционных систем	Содержание учебного материала	20
	1. Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. WindowsXP. Windows 7. Windows8. Linux. QNX и другие операционные системы.	
	2. Технологии аутентификации.	
	3. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации	
	4. Пароли. PIN-коды. Методы надежного составления паролей.	
	5. Строгая аутентификация.	
	6. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи.	
	7. Программно-аппаратные модули доверенной загрузки.	
	8. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ.	
	9. АПМДЗ Криптон –Замок системный администратор.	
	10. Изучение настроек системного администратора АПМДЗ.	
	11. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ.	
	12. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ.	
	Практические занятия	
	Изучение средств идентификации аутентификации операционных систем	2
	Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя.	
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита.	2
	Настройка изолированной среды.	2

	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды.	2
	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	2
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	2
	Восстановление информации типовыми средствами Программы восстановление информации	2
Тема1.2. Технологии разграничения доступа	Содержание учебного материала	
	<ol style="list-style-type: none"> 1. Архитектура подсистемы защиты операционной системы Windows Server2016. 2. Особенности ОС Windows Server2016. Возможности администратора. Разграничение доступа к объектам операционной системы. 3. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. 4. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда. 5. Способы организации. Методы применения. 6. ActiveDirectory. 7. Комплексная система организации управления доступом. Инсталляция. Настройка. 8. Аудит безопасности операционной системы. 9. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. 10. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 11. Особенности функционирования межсетевых экранов. 12. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. 13. Схемы защиты на базе межсетевых экранов. 14. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. 15. Тестирование межсетевых экранов. 16. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. 	25
	Практические занятия	
	Программы надежного удаления информации.	2

	Архивирование информации.	2
	Программные средства резервного копирования. Настройка RAID-массивов.	2
	Инсайдерская информация. Программы сбора информации о ПК.	2
	Настройка межсетевого экрана.	2
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Содержание учебного материала	
	1. Проблемы информационной безопасности сетей. 2. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек 3. протоколов TCP/IP. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. 4. Концепция построения виртуальных защищенных сетей. 5. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. 6. VPN – решения для построения защищенных сетей. 7. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. 8. Протоколы PPTP, L2F, L2TP. 9. Протоколы формирования защищенных каналов на сеансовом уровне. 10. Протоколы SSL, TLS, SOCKS. 11. Защита на сетевом уровне. 12. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. 13. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом. Web-доступ. Протоколы PAP, CHAP, S/Key, SSO, Kerberos.	25
	Практические занятия	
	Основные действия с виртуальной машиной	1
	Работа с контрольными точками	1
	Использование внешних устройств	1
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	1
	Установка и настройка ПО eTokenPKIClient	1
	Настройка ПО eTokenPKIClient с помощью групповых политик	1
	Развертывание TMS в среде Active Directory	1

	Настройка TMS в среде Active Directory	1
	Настройка политик TMS	1
	Настройка использования виртуального токена	1
	Использование токена на рабочем месте администратора	2
	Установка и настройка СКЗИ «КриптоПроCSP»	2
	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	2
	Применение SecretDisk4	2
	Применение SecretDisk Server NG	2
	Изучение основных возможностей ПО VipNetClient	2
	Изучение настроек ПО VipNetClient	2
	Изучение возможностей ПО Деловая почта	2
	Изучение средств обнаружения атак	2
	Изучение антивирусных продуктов	2
Тема 1.4. Методы управления средствами защиты	Содержание учебного материала	10
	1. Методы управления средствами сетевой защиты. 2. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. 3. Функционирование системы управления средствами защиты. 4. Аудит безопасности информационной системы. 5. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. 6. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	
Самостоятельная работа при изучении МДК 02.01		100
Рекомендуемая примерная тематика внеаудиторной самостоятельной работы:		
1. Проблемы обеспечения безопасности операционных систем WindowsXP. Windows 7. Windows8. Linux. QNX. 2. Технологии аутентификации. 3. Аутентификация, авторизация и администрирование действий пользователя. 4.Пароли. PIN-коды. Методы надежного составления паролей. 4. Токены. Смарт-карты. Виртуальные ключи. 5. Программно-аппаратные модули доверенной загрузки. 6. АПМДЗ Криптон –Замок системный администратор. 7. Изучение настроек системного администратора АПМДЗ.		

8. Сектор НЖМД. Область памяти. Файл, папка, каталог.
9. Разграничение доступа к объектам операционной системы.
10. Комплексная система организации управления доступом. Инсталляция. Настройка. 12.Аудит безопасности операционной системы.
11. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 14.Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ.
12. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ.
13. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.
14. Концепция построения виртуальных защищенных сетей;.
15. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов.
16. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP.
17. Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS.
18. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP.
19. Защита на прикладном уровне. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.3.сыМЭ. Требования ФСТЭК к МЭ документацию на оборудование ИТКС.
20. Функционирование системы управления средствами защиты.
21. Аудит безопасности информационной системы.

Курсовые работы (проекты)	20
<p>Тематика курсовых работ (проектов):</p> <ol style="list-style-type: none"> 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. 	

Промежуточная аттестация в форме экзамена		10
Всего по МДК 02.01		244
МДК 02.02. Криптографическая защита информации		102
Тема 2.1. Основы криптографических методов защиты информации	Содержание учебного материала	
	1. Свойства информационной безопасности. 2. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. 3. Криптографические методы. 4. Шифрование. Кодирование. Стеганография. Сжатие. 5. Математика криптографии. 6. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. 7. Традиционные шифры перестановки. 8. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. 9. Традиционные шифры замены. 10. Шифры замены. Шифры многоалфавитной замены. Частотность символов. 11. Криптоанализ. 12. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 13. Компьютерное шифрование. 14. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	14
	Практические занятия	
	Стеганографические методы скрытия информации	2
	Бинарная арифметика. Модульная арифметика	2
	Применение методов шифрования перестановкой	2
	Применение методов шифрования заменой	2
	Применение методов шифрования многоалфавитной замены	2
	Криптоанализ методов перестановки	2
	Криптоанализ методов замены	2
	Компьютерное шифрование	2
Тема 2.2. Современные стандарты шифрования	Содержание учебного материала	
	1. Симметричное шифрование.	14

	<p>2. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES.</p> <p>3. Усовершенствованный стандарт шифрования AES.</p> <p>4. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES.</p> <p>5. Российские стандарты симметричного шифрования .</p> <p>6. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147- 89. ГОСТ Р 34.12-2015.</p> <p>7. Проблема распределения ключей симметричного шифрования.</p> <p>8. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование.</p> <p>9. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамала. Криптосистемы на основе метода эллиптических кривых. ЭЦП.</p> <p>10. Российские стандарты асимметричного шифрования.</p> <p>11. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.</p>	
	Практические занятия	
	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	2
	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	2
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	Содержание учебного материала	
	<p>1. Целостность сообщения.</p> <p>2. Случайная модель Огасле. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции.</p> <p>3. Электронная цифровая подпись.</p> <p>4. Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012.</p> <p>5. Установление подлинности объекта.</p> <p>6. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены.</p> <p>7. Проблемы распределения открытого ключа асимметричного шифрования.</p>	18

	8. Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI.		
	9. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне.		
	10. Электронная почта. Архитектура e-mail. PGP. S/MIME .		
	11. Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне.		
	12. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети Защита информации в сетях, организованных по технологии беспроводного доступа.		
	13. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16.		
	14. Защита информации в сетях сотовой связи. A3. A8.A5/3. Атаки на алгоритмы.		
	15. Перспективы развития беспроводной мобильной связи. Криптовалюты.		
	16. Биткоин. Блокчейн-системы Ethereum.		
	17. Перспективы развития криптографии.		
	18. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории ассиметричных алгоритмов		
	Практические занятия		
	Разработка хэш-функции		2
	Разработка схемы простого пароля		2
	Разработка схемы динамического пароля		2
	Сертификаты открытого ключа		2
	Настройка и администрирование токена		2
	Настройка сервисов Рутокен-PinPad		2
	Настройка сервисов Рутокен-ЭЦП	2	
	Настройка сервисов Рутокен-Bluetooth	2	
Настройка сервисов Рутокен-S	2		
Разработка алгоритма PGP	2		
Изучение протоколов SSL, TLS, IPSec	2		
Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	2		
Самостоятельная работа		60	
Рекомендуемая тематика самостоятельной работы			
1. Изучение новых технологий хранения информации.			
2. Статистика и анализ крупных утечек информации за год.			
3. Поиск информации о новых видах атак на информационную систему.			

4. Обзор современных программных и программно-аппаратных средств защиты. 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты. 6. Криптографические методы. 7. Шифрование. Кодирование. Стеганография. Сжатие. 8. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. 9. Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов. 10. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 11. Компьютерное шифрование. 12. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 13. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. 14. Асимметричное шифрование. Криптографическая система Эль-Гамала. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.	
Промежуточная аттестация в форме дифференцированного зачета	2
Всего по МДК 02.02	150
Учебная практика (по профилю специальности) итоговая по ПМ Виды работ Выбор, подключение, настройка межсетевого экрана. Администрирование межсетевого экрана. Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования. Ознакомление, подключение, настройка системы антивирусной защиты. Администрирование системы антивирусной защиты. Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции Составление алгоритма шифра Подключение, установка драйверов, настройка программных средств шифрования Криптон. Администрирование программных средств шифрования Криптон Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. Администрирование аппаратных средств шифрования Криптон.	36
Производственная практика (по профилю специальности) итоговая по ПМ Виды работ Участие в организации работ по защите персональных компьютеров на предприятии Участие в организации работ по защите локальных сетей на предприятии Участие в организации работ по защите работ в глобальной сети интернет на предприятии Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети.	144

Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей Подключение, установка драйверов, настройка программных средств абонентского шифрования Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств РКІ	
КВАЛИФИКАЦИОННЫЙ ЭКЗАМЕН ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ 02	20
Всего по ПМ 02:	
Теоретических занятий	150
Практических занятий	110
Самостоятельной работы	184
Учебная практика	36
Производственная практика	144
Экзамен по ПМ 02	20
ИТОГО	654

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения (в соответствии с ФГОС и ПООП):

1. Лаборатория программных и программно-аппаратных средств защиты информации

Специализированная мебель:

Лекционные парты – 26 шт.

Стулья – 53 шт.

Стол компьютерный – 1 шт.

Учебная доска – 1 шт.

Экран настенный – 1 шт.

Технические средства обучения:

Компьютер преподавателя – 1 шт

Мультимедиа проектор – 1 шт.

Аудиоколонки – 1шт

Сервер – 2 шт.

Источники бесперебойного питания – 2 шт.

Многофункциональное устройство -1 шт.

Антивирусные программные комплексы; аппаратные средства аутентификации пользователя; программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации; средства защиты информации от несанкционированного доступа, блокирования доступа и нарушения целостности; программные средства криптографической защиты информации; программные средства выявления уязвимостей и оценки защищенности информационно-телекоммуникационной системы, анализа сетевого трафика.

Перечень лицензионного программного обеспечения:

1) Антивирусная защита Kaspersky Endpoint Security

2) Astra Linux, Libre Office

3) Программные средства криптографической защиты информации

4) Программно-аппаратные средства управления доступом к данным и защиты (шифрования) информации, средствами защиты информации от НСД, блокирования доступа и нарушения целостности;

Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде Финансового университета.

2. Лаборатория защиты информации от утечки по техническим каналам

Специализированная мебель:

Стол письменный – 19 шт.

Стулья – 48 шт.

Стол переговорочный – 2 шт.

Стол компьютерный – 1 шт.

Технические средства обучения:

Стенды физической защиты объектов информатизации – 2 шт.

Компьютер преподавателя – 1 шт
Мультимедиа проектор – 1 шт.
Экран настенный – 1 шт
Аудиоколонки – 1шт

Средства защиты информации от утечки по акустическому (виброакустическому) каналу; средства защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средства контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок.

Перечень лицензионного программного обеспечения:

- 1) Антивирусная защита Kaspersky Endpoint Security
- 2) Astra Linux, Libre Office
- 3) СПС «Гарант»

Помещение обеспечено доступом к сети «Интернет» и электронной информационно-образовательной среде Финансового университета.

3. Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
(Методический кабинет)

Специализированная мебель:

Компьютерные столы – 20 шт.
Стол письменный – 13 шт.
Кресло компьютерное – 20 шт.
Стулья – 26 шт.
Шкаф для учебно-методических материалов – 6 шт.

Технические средства обучения:

Персональные компьютеры – 18 шт.
Мультимедиа проектор – 1 шт.
Экран настенный – 1 шт.
Аудиоколонки – 1шт.

4. Помещения для самостоятельной работы: Библиотека и читальный зал с выходом в сеть Интернет

Специализированная мебель:

Стол кафедра – 3 шт.
Каталожный ящик – 1 шт.
Шкаф для читательских формуляров – 3 шт.
Витрина для книг – 3 шт.
Стол ученический – 24 шт.
Кресло компьютерное – 2 шт.
Стул - 48 шт.
Стол эргономичный с тумбой – 1 шт.
Шкаф для документов – 3 шт.

Технические средства обучения:

Персональные компьютеры– 18 шт.

Реализация профессионального модуля предполагает обязательную учебную и производственную практику (по профилю специальности). Учебная практика проводится концентрированно в учебном заведении, производственная практика (по профилю специальности) проводится концентрированно в организациях работодателей, с которыми заключены договоры о практической подготовке обучающихся.

3.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации имеет электронные издания и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Сети и телекоммуникации: учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 464 с. — ISBN 978-5-534-17315-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://ezpro.fa.ru:2058/bcode/536089> (дата обращения: 22.08.2024)

2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – Спб.: Питер, 2020. – 1008 с.

3. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учебное издание / Белов Е.Б., Пржегорлинский В. Н. - Москва : Академия, 2021. - 336 с. (Специальности среднего профессионального образования). - URL: <https://academia-moscow.ru> - Режим доступа: Электронная библиотека «Academia-moscow». - Текст : электронный

4. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2107178> (дата обращения: 22.08.2024).

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

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

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

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

Федеральный портал «Информационно- коммуникационные технологии в образовании» <http://www.ict.edu.ru>

<http://www.morion.ru/>

<http://www.nateks.ru/>

<http://www.iskratel.com/>

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

<http://3m.com/>

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

3.2.3. Дополнительные источники

Дополнительные источники:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

- Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
- Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
- Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
- ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
- ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
- ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
- ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
- ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
- ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Отечественные журналы:

"InformationSecurity/ Информационная безопасность"

Системный администратор

Компьютер ПРЕСС

Системы безопасности. Журнал для руководителей и специалистов в области безопасности

- Сети и системы связи
- Защита информации. Инсайд: Информационно-методический журнал
- Информационная безопасность регионов: Научно-практический журнал

Интернет-ресурсы:

<http://cryptogrof.ru/>

В соответствии со ст. 43 Конституции Российской Федерации, 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012, приказом Минобрнауки России от 09.11.2015 N 1309 «Об

утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», ГОСТ Р 57723-2017 «Информационно-коммуникационные технологии в образовании. Системы электронно-библиотечные. Общие положения», ГОСТ Р 52872-2019 «Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности», все предлагаемые электронные ресурсы максимально комфортны для чтения слабовидящими людьми. Масштабирование текста достигает 300 процентов. При изменении масштаба сохраняется возможность видеть всю страницу текста, не обрезая его.

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. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей.	<ul style="list-style-type: none"> - 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. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	<ul style="list-style-type: none"> - 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. Осуществлять защиту информации от несанкционированных действий 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.	<ul style="list-style-type: none"> - 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, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	<ul style="list-style-type: none"> - демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы; 	Экспертное наблюдение Экзамен
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	<ul style="list-style-type: none"> - 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. Пользоваться профессиональной документацией на государственном и иностранном языках.	<ul style="list-style-type: none"> - эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; 	Экспертное наблюдение Экзамен