МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

УТВЕРЖДАЮ
зам. директора по УМР
_____С.А. Косова
«02» 06 2023 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

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

г. Шатура
2023 г.

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Краснолобов Дмитрий Михайлович, преподаватель специальных дисциплин

Еремина Елена Алексеевна, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС Информатика и вычислительная техника и Информационная безопасность (09.02.06, 10.02.04)

Протокол № 11 от «01» 06 2023 г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Е.В. Лялина, методист ГБПОУ МО «ШЭТ»

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. 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 профессиональные компетенции:

1.1.1 Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих

ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР 19	Готовый к профессиональной конкуренции и конструктивной реакции на критику.

1.1.2 Перечень профессиональных компетенций

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

1.1.3 В результате освоения профессионального модуля студент должен:

Иметь практический опыт	• определения необходимых средств криптографической защиты информации; • использования программно-аппаратных криптографических средств защиты информации; • установки, настройки специализированного оборудования криптографической защиты информации; • применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; • шифрования информации.
Уметь	• Выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; • определять рациональные методы и средства защиты на объектах и оценивать их эффективность; • производить установку и настройку типовых программно-аппаратных средств защиты информации; • пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации.
Знать	• Типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; • основные протоколы идентификации и аутентификации в телекоммуникационных системах; • состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; • особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; • основные способы противодействия несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; • основные понятия криптографии и типовые криптографические методы защиты информации.

1.2. Количество часов, отводимое на освоение профессионального модуля.

Всего 573 часов, в том числе в форме практической подготовки 563 часов.

Из них:

на освоение МДК 02.01 215 часов;

МДК 02.02 98 часов;

в том числе, самостоятельная работа - 2 часа

курсовой проект – 30 часов

на практики, в том числе:

учебную – 108 часов

производственную – 144 часа

Промежуточная аттестация – 17 часов, в том числе:

экзамены, дифференцированные зачеты и консультации – 9 часов,

экзамен по модулю - 8 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля.

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					Самостоятельная работа[1]
			Обучение по МДК			Практики		
			всего, часов	Лабораторных и практических занятий	Курсовых работ (проектов)*	Учебная	Производственная	
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7, 14, 19	МДК 02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»	**215**	215	88	30	-	-	-
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7, 14, 19	МДК 02.02 «Криптографическая защита информации»	**98**	96	44	-	-	-	2
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7, 14, 19	Учебная практика	**108**	-	-	-	108	-	-

[1]Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7, 14, 19	Производственная практика	**144**	
	Промежуточная аттестация	**8**	8
	Всего:	**573**	**3**

-	-	-	-	144	-
8	-	-	-	-	-
19	**132**	**30**	**108**	**144**	**2**

2.2. Тематический план и содержание профессионального модуля.

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
1	2	3
ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты»		**573**
МДК 02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»		**215**
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание:** • Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows 10. Linux. QNX и другие операционные системы. • Технологии аутентификации. • Аутентификация, авторизация и администрирование действий пользователя. • Методы аутентификации • Пароли. PIN-коды. Методы надежного составления паролей. • Строгая аутентификация. • Односторонняя аутентификация. Двухсторонняя аутентификация. • Аппаратно-программные средства идентификации и аутентификации. • Токены. Смарт-карты. Виртуальные ключи. • Программно-аппаратные модули доверенной загрузки. • Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. • АПМДЗ Криптон – Замок системный администратор.	**24**

	• Изучение настроек системного администратора АПМДЗ. • АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ. • Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ. • Сектор НЖМД. Область памяти. Файл, папка, каталог.	
	Практические и лабораторные работы	**22**
	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя	**4**
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	**4**
	Настройка изолированной среды	**2**
	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	**4**
	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	**4**
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	**2**
	Восстановление информации типовыми средствами Программы восстановление информации	**2**
Тема 1.2. Технологии разграничения доступа	**Содержание:**	**30**
	• Архитектура подсистемы защиты операционной системы Windows Server2016. • Особенности ОС Windows Server2016. Возможности администратора. • Разграничение доступа к объектам операционной системы. • Модели доступа. Дискреционная модель. Мандатная модель. Роли. • Локальная политика безопасности.	

	• Настройка локальной политики безопасности. Администрирование системы. • Изолированная программная среда. • Способы организации. Методы применения. • ActiveDirectory. • Комплексная система организации управления доступом. Инсталяция. Настройка. • Аудит безопасности операционной системы. • Методы проведения контрольных проверочных мероприятий. Программные средства аудита. • Функции межсетевых экранов. • Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. • Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. • Особенности функционирования межсетевых экранов. • Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. • Схемы защиты на базе межсетевых экранов. • Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. • Тестирование межсетевых экранов. • Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.	
	Практические и лабораторные работы	**16**
	Программы надежного удаления информации	**2**

	Архивирование информации	**4**
	Программные средства резервного копирования. Настройка RAID-массивов	**4**
	Инсайдерская информация. Программы сбора информации о ПК	**2**
	Настройка межсетевого экрана.	**4**
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание:** • 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. • Концепция построения виртуальных защищенных сетей. • Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. • VPN – решения для построения защищенных сетей. • Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. • Защита на канальном уровне. • Протоколы PPTP, L2F, L2TP. • Протоколы формирования защищенных каналов на сеансовом уровне. • Протоколы SSL, TLS, SOCKS. • Защита на сетевом уровне. • Архитектура средств безопасности IPSec, AH, ESP. • Защита на прикладном уровне.	**20**

	• Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом.Web-доступ. Протоколы PAP, CHAP,S/Key, SSO, Kerberos.	
	Практические и лабораторные работы	**42**
	Основные действия с виртуальной машиной	**4**
	Работа с контрольными точками	**4**
	Использование внешних устройств	**2**
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	**2**
	Установка и настройка ПО eTokenPKIClient	**2**
	Настройка ПО eTokenPKIClient с помощью групповых политик	**2**
	Развертывание TMS в среде Active Directory	**2**
	Настройка TMS в среде Active Directory	**2**
	Настройка политик TMS	**4**
	Настройка использования виртуального токена	**2**
	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**
Тема 1.4. Технологии обнаружения вторжений	**Содержание:**	**10**
	• Технология обнаружения атак.	

	• Концепция адаптивного управления безопасностью. Технология анализа защищенности. • Средства анализа защищенности сетевых протоколов и сервисов. • Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. • Средства обнаружения сетевых атак. • Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки. • Обзор современных средств обнаружения атак. • Технологии защиты от вирусов. • Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.	
	Практические и лабораторные работы	**8**
	Изучение средств обнаружения атак	**4**
	Изучение антивирусных продуктов	**4**
Тема 1.5. Методы управления средствами защиты	**Содержание:**	**8**
	• Методы управления средствами сетевой защиты. • Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. • Аудит безопасности информационной системы. • Мониторинг безопасности системы. Программные средства проведения аудита безопасности.	

	• Обзор современных систем управления сетевой защитой. • Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.	
Курсовой проект (работа). **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. 15. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 16. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей. 17 .Анализ методов и средств анализа защищенности беспроводных сетей. 18. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 19. Виброакустические средства современных систем обеспечения информационной безопасности.		**30**

20. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 21. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 22. Средства обеспечения информационной безопасности банков данных. 23. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 24. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 25. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 26. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 27. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 28. Инструментальные средства анализа рисков информационной безопасности. 29. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 30. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).		
Учебная практика раздела МДК 02.01. **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.		**36**
МДК 02.02 «Криптографическая защита информации»		**98**
Тема 2.1. Основы криптографических методов защиты информации	**Содержание:**	**26**
	• Свойства информационной безопасности.	

	• Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. • Криптографические методы. • Шифрование. Кодирование. Стеганография. Сжатие. • Математика криптографии. • Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. • Традиционные шифры перестановки. • Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. • Традиционные шифры замены. • Шифры замены. Шифры многоалфавитной замены. Частотность символов. • Криптоанализ. • Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. • Компьютерное шифрование. • Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	
	Практические и лабораторные работы	**16**
	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:**	**22**
	• Симметричное шифрование. • Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. • Усовершенствованный стандарт шифрования AES. • Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. • Российские стандарты симметричного шифрования. • Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. • Проблема распределения ключей симметричного шифрования. • Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. • Асимметричное шифрование. • Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. • Российские стандарты асимметричного шифрования. • ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.	
	Практические и лабораторные работы	**4**
	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:** • Целостность сообщения. • Случайная модель Oracle. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции. • Электронная цифровая подпись. • Алгоритм формирования подписи. Свойства, обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012. • Установление подлинности объекта. • Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. • Проблемы распределения открытого ключа асимметричного шифрования. • Сертификаты открытого ключа. Удостоверяющие центры. X.509. Иерархия PKI. • Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. • Электронная почта. Архитектура e-mail. PGP. S/M1ME. • Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. • Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети • Защита информации в сетях, организованных по технологии беспроводного доступа. • IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16.	**28**

	• Защита информации в сетях сотовой связи. • А3. А8.А5/3. Атаки на алгоритмы. • Перспективы развития беспроводной мобильной связи. • Криптовалюты. • Биткоин. Блокчейн-системы Ethereum. • Перспективы развития криптографии. • Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.	
	Практические и лабораторные работы	**24**
	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 учебная работа при изучении раздела МДК 02.02. **Рекомендуемая тематика внеаудиторной (самостоятельной) работы:** • Статистика и анализ крупных утечек информации за год. • Поиск информации о новых видах атак на информационную систему. • Обзор современных программных и программно-аппаратных средств защиты.	**2**
Учебная практика раздела МДК 02.02. **Виды работ:** • Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции. • Составление алгоритма шифра. • Подключение, установка драйверов, настройка программных средств шифрования Криптон. • Администрирование программных средств шифрования Криптон • Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. • Администрирование аппаратных средств шифрования Криптон.	**72**
Производственная практика. **Виды работ:** • Участие в организации работ по защите персональных компьютеров на предприятии. • Участие в организации работ по защите локальных сетей на предприятии. • Участие в организации работ по защите работ в глобальной сети интернет на предприятии. • Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. • Администрирование систем безопасности проводной защищенной локальной сети. • Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. • Администрирование систем безопасности беспроводной защищенной локальной сети. • Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. • Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей.	**144**

• Подключение, установка драйверов, настройка программных средств абонентского шифрования. • Администрирование внедренных средств. • Настройка средств электронной подписи. • Администрирование средств электронной подписи. • Администрирование средств PKI.	
Промежуточная аттестация	**8**
Всего	**573**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы профессионального модуля требует наличия учебных кабинетов, лабораторий:

1. Лаборатория «Программных и программно-аппаратных средств защиты информации». Лаборатория должна быть 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 обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

3.2.1. Печатные издания:

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

2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – Спб.: Питер, 2017. – 992 с.

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

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2017. – 184 с.

5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2017. – 172 с.

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

3.2.2. Электронные издания (электронные ресурсы):

Интернет-ресурсы:

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

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

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

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

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

3.2.3. Дополнительные источники:

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

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

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

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

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

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

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

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

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

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с

постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

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

12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

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

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

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

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

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

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

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

21. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

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

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

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

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

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

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

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

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

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

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

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

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

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

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

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

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по

защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

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

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

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

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

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

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

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

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 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 - 2.3 **ОК 1-10** **ЛР 3, 4, 7, 14, 19**	«отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко; «хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками; «удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки; «неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: - на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.); - при выполнении и защите курсовой работы (проекта); - при выполнении работ на различных этапах производственной практики; - при проведении: контрольных работ, зачетов, экзаменов по междисциплинарным курсам, экзамена (квалификационного) по модулю.