Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«**Колледж автоматизации производственных процессов
и прикладных информационных систем**»

Рассмотрена и принята
на заседании Педагогического совета
Протокол №9 от 15.05.2026 г.

УТВЕРЖДЕНА
Приказом директора
СПб ГБПОУ «Колледж
автоматизации производства»
от 15.05.2026 г. №624

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

Для специальности **10.02.05 «Обеспечение информационной безопасности автоматизированных систем»**

Квалификация специалиста базовой подготовки	техник по защите информации
Форма обучения	очная
Уровень образования, необходимый для приема на обучение по ППССЗ	основное общее образование
Срок получения СПО по ППССЗ базовой подготовки	3 года 10 месяцев
Год начала подготовки	2024

Санкт-Петербург

Рабочая программа разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553

Организация-разработчик: Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Колледж автоматизации производственных процессов и прикладных информационных систем»

Программу составили: Крамсакова А.М., Казакова Н.В., преподаватели СПб ГБПОУ «Колледж автоматизации производственных процессов и прикладных информационных систем».

Программа рассмотрена и одобрена на заседании методической комиссии, протокол №08 от 27.04.2026 г.

Заведующий отделом СОП А.Ф. Жмайло

С О Д Е Р Ж А Н И Е

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПМ.02 4
1.1. Область применения программы 4
1.2. Цели и задачи модуля – требования к результатам освоения модуля 4
1.3. Планируемое количество часов на освоение программы ПМ.02: 5
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 6
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 7
3.1. Тематический план профессионального модуля 7
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ 16
4.1. Требования к минимальному материально-техническому обеспечению 16
4.2. Информационное обеспечение обучения 16
4.3. Общие требования к организации образовательного процесса 17
4.4. Кадровое обеспечение образовательного процесса 17
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ) 18

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПМ.02
«Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью ППССЗ в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» в части освоения основного вида профессиональной деятельности (ВПД): «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями учащийся в ходе освоения профессионального модуля должен:

уметь:

- устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;
- использовать типовые программные криптографические средства, в том числе электронную подпись;
- устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;
- осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

знать:

- особенности и способы применения программных и программно-аппаратных

средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
- типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации.

иметь практический опыт в:
- установке и настройке программных средств защиты информации;
- тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;
- учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

1.3. Планируемое количество часов на освоение программы ПМ.02:

№	Вид учебной работы	Объем часов
1.	**Объем работы обучающихся во взаимодействии с преподавателем**	**734**
в том числе:		
теоретическое обучение		160
практические занятия		176
учебная практика		36
производственная практика		324
Промежуточная аттестация в форме экзамена		**18**
2.	**Самостоятельная внеаудиторная работа обучающихся**	**42**
Всего по ПМ.02 в рамках образовательной программы		**776**

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», в том числе профессиональными (ПК) и общими (ОК) компетенциями.

Код	Наименование результата обучения
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
ПК 2.6	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
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 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды ОК, ПК	Наименования разделов профессионального модуля	Общий объем нагрузки, акад. час	В форме практической подготовки	Объем профессионального модуля, акад. час					
				Работа обучающихся во взаимодействии с преподавателем					Самостоятельная работа
				Всего	в том числе				
					лабораторные и практические занятия	курсовая работа, проект	учебная практика	производственная практика	
1	2	3	4	5	6	7	8	9	10
ОК 01- 09 ПК 2.1. – 2.6	Раздел 1. Программные и программно-аппаратные средства защиты информации	278	154	248	134	20			30
ОК 01- 09 ПК 2.2, ПК 2.4	Раздел 2. Криптографические средства защиты информации	120	42	108	42				12
УП.02	Учебная практика	36	36	36			36		
ПП.02	Производственная практика	324	324					324	
	Промежуточная аттестация	18	18	18					
	Итого	776	574	374	176	20	36	324	42

3.2. Содержание обучения по профессиональному модулю ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами»

Таблица 4

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 всего
Раздел 1 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		
МДК 02.01 Защита информации в автоматизированных системах программными и программно-аппаратными средствами		**248**
Тема 1.1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности	**Содержание учебного материала**	**18**
	1.1.1. Особенности и способы применения программных и программно-аппаратных средств защиты информации	
	1.1.2 Анализ угроз информационной безопасности	
	1.1.3 Анализ сетевых угроз информационной безопасности	
	1.1.4 Классификация программно-аппаратных средств обеспечения информационной безопасности	
	1.1.5 Функциональные возможности программно-аппаратных средств обеспечения информационной безопасности	
	1.1.6 Требования регуляторов по защите информации в автоматизированных системах	
	1.1.7 Обзор отечественных продуктов для централизованного управления пользователями и рабочими станциями	
	1.1.8 Возможности групповых политик при администрировании всех устройств и пользователей	
	1.1.9 Понятие журналирования в операционных системах Windows и Linux	
	Практические занятия	**24**
	Практическое занятие № 1 Установка серверной версии Windows, АРМ на Windows. Установка Linux для сервера и клиента	
	Практическое занятие № 2 Поднятие AD	
	Практическое занятие № 3 Добавление рабочих станций в домен AD	
	Практическое занятие № 4 Применение групповых политик AD	
	Практическое занятие № 5 Подготовка отечественной ОС для поднятия сервера	

	Практическое занятие № 6 Поднятие сервера на отечественной ОС	
	Практическое занятие № 7 Настройка доверительных отношений между серверами	
	Практическое занятие № 8 Добавление рабочих станций на сервер Linux	
	Практическое занятие № 9 Создание групповых политик на сервере Linux	
	Практическое занятие № 10 Применение групповых политик на сервере Linux	
	Практическое занятие № 11 Журналирование действий на Windows	
	Практическое занятие № 12 Журналирование действий на Linux	
Тема 1.2 Методы и средства реализации функциональных требований по защите информации и данных	**Содержание учебного материала**	**14**
	1.2.1 Основные принципы разграничения доступа к ресурсам	
	1.2.2 Методы обнаружения компьютерных вирусов	
	1.2.3 Методы обеспечения целостности системы защиты	
	1.2.4 Резервирование данных	
	1.2.5 Методы криптографической защиты информации	
	1.2.6 Применение электронной цифровой подписи	
	1.2.7 Понятие хеширования данных	
	Практические занятия	**34**
	Практическое занятие № 13 Применение антивирусного программного обеспечения на ОС Windows	
	Практическое занятие № 14 Применение антивирусного программного обеспечения на ОС Linux	
	Практическое занятие № 15 Установка системы бэкап	
	Практическое занятие № 16 Система бэкап: создание резервной копии всего содержимого компьютера	
	Практическое занятие № 17 Система бэкап: создание загрузочного носителя	
	Практическое занятие № 18 Система бэкап: создание пакета «всё в одном» для восстановления данных	
	Практическое занятие № 19 Система бэкап: архивирование данных	
	Практическое занятие № 20 Установка средства доверенной загрузки	
	Практическое занятие № 21 Настройка параметров безопасности средства доверенной загрузки	
	Практическое занятие № 22 Управление функционированием механизмов защиты на компьютерах с помощью средства доверенной загрузки	
	Практическое занятие № 23 Работа с централизованными журналами в средстве доверенной загрузки	
	Практическое занятие № 24 Формирование отчётов в средстве доверенной загрузки	
	Практическое занятие № 25 Установка криптопровайдера	
	Практическое занятие № 26 Работа с сертификатами в режиме командной строки в криптопровайдере	
	Практическое занятие № 27 Работа с ЭЦП в режиме командной строки	
	Практическое занятие № 28 Шифрование данных в режиме командной строки	

	Практическое занятие № 29 Хеширование данных и проверка их целостности в режиме командной строки	
Тема 1.3 Программно-аппаратные средства защиты информации в операционных системах и базах данных	**Содержание учебного материала**	**16**
	1.3.1 Понятие и назначение изолированной программной среды	
	1.3.2 Понятие и назначение автоматизированного аудита файловой системы	
	1.3.3 Подсистема безопасности Windows и Linux	
	1.3.4 Обеспечение безопасности СУБД	
	1.3.5 Принцип работы системы предотвращения утечек конфиденциальной информации в информационных системах организации	
	1.3.6 Понятие объектов защиты. Принципы написания политик безопасности DLP-систем	
	1.3.7 Принципы построения регулярных выражений. Мониторинг событий DLP-системы	
	1.3.8 Критерии защищённости информационных систем.	
	Практические занятия	**48**
	Практическое занятие № 30 Установка и настройка замкнутой программной среды	
	Практическое занятие № 31 Применение замкнутой программной среды	
	Практическое занятие № 32 Установка DCAP-системы	
	Практическое занятие № 33 DCAP-система: анализ и категоризация содержимого файлов	
	Практическое занятие № 34 DCAP-система: мониторинг прав доступа пользователей к файлам	
	Практическое занятие № 35 DCAP-система: поиск файлов по всем хранилищам данных	
	Практическое занятие № 36 Установка средства защиты данных в СУБД	
	Практическое занятие № 37 Настройка средства защиты данных в СУБД	
	Практическое занятие № 38 Применение средства защиты данных в СУБД	
	Практическое занятие № 39 Установка DLP-системы	
	Практическое занятие № 40 Установка веб-консоли DLP-системы	
	Практическое занятие № 41 Установка сервера DLP-системы	
	Практическое занятие № 42 Установка сертификатов для совместной работы серверов DLP-системы	
	Практическое занятие № 43 Защита HTTPS-соединения с DLP-системой. Создание цифровых сертификатов	
	Практическое занятие № 44 Беспарольное SSH-соединение защищенного доступа к серверу DLP-системы	
	Практическое занятие № 45 Установка агентов безопасности на машины нарушителей	
	Практическое занятие № 46 Создание и применение правил в DLP-системе, запрещающих доступ к устройствам	
	Практическое занятие № 47 Создание и применение правил в DLP-системе, контролирующих копирование информации на различные носители	

	Практическое занятие № 48 Создание и применение правил в DLP-системе для теневого копирования	
	Практическое занятие № 49 Создание и применение политик в DLP-системе с использованием встроенных объектов защиты	
	Практическое занятие № 50 Создание и применение политик в DLP-системе с использованием своих объектов защиты	
	Практическое занятие № 51 Создание и применение политик в DLP-системе с использованием графических объектов	
	Практическое занятие № 52 Создание и применение политик в DLP-системе с использованием регулярных выражений	
	Практическое занятие № 53 Создание сводок и отчётов в DLP-системе	
Тема 1.4 Программно-аппаратные средства защиты информации в сетях передачи данных	**Содержание учебного материала**	**14**
	1.4.1 Принципы построения и функционирования межсетевых экранов	
	1.4.2 Основные принципы защиты информации при передаче по каналам связи	
	1.4.3 Защищенные протоколы передачи данных	
	1.4.4 Основные принципы обнаружения сетевых атак	
	1.4.5 Программно-аппаратные средства защиты от сетевых атак	
	1.4.6 Средства анализа защищенности	
	1.4.7 Основы тестирования на проникновение. Этапы тестирования на проникновение	
	Практические занятия	**48**
	Практическое занятие № 54 Первичная настройка промышленного межсетевого экрана	
	Практическое занятие № 55 Работа в веб-интерфейсе межсетевого экрана	
	Практическое занятие № 56 Настройка правил межсетевого экрана	
	Практическое занятие № 57 Проверка созданных правил межсетевого экрана	
	Практическое занятие № 58 Настройка ограничения трафика с помощью МЭ	
	Практическое занятие № 59 Настройка отказоустойчивого кластера МЭ	
	Практическое занятие № 60 Настройка МЭ в качестве СОВ	
	Практическое занятие № 61 Создание пользовательских правил на основе собственного шаблона	
	Практическое занятие № 62 Проверка созданных правил СОВ	
	Практическое занятие № 63 Настройка прокси-сервера с помощью межсетевого экрана	
	Практическое занятие № 64 Создание правил запрета обхода трафика на МЭ и эмуляция атак	

	Практическое занятие № 65 Развёртывание защищённой виртуальной сети	
	Практическое занятие № 66 Создание структуры защищённой виртуальной сети	
	Практическое занятие № 67 Создание связей, настройка координаторов в защищённой виртуальной сети	
	Практическое занятие №68 Развёртывание рабочего места помощника главного администратора защищённой сети	
	Практическое занятие № 69 Модификация защищённой виртуальной сети	
	Практическое занятие № 70 Компрометация ключей в защищённой виртуальной сети	
	Практическое занятие № 71 Настройка политик безопасности в защищённой виртуальной сети	
	Практическое занятие № 72 Организация межсетевого взаимодействия	
	Практическое занятие № 73 Модификация межсетевого взаимодействия в защищённой виртуальной сети	
	Практическое занятие № 74 Настройка работы удостоверяющего центра в аккредитованном режиме	
	Практическое занятие № 75 Работа с сервером установки штампа времени	
	Практическое занятие № 76 Настройка правил в защищённой виртуальной сети	
	Практическое занятие № 77 Туннелирование в рамках межсетевого взаимодействия в защищённой виртуальной сети	
Тема 1.5 Сертификация программно-аппаратных средств обеспечения информационной безопасности	**Содержание учебного материала**	**6**
	1.5.1 Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности	
	1.5.2 Классификация требований к программно-аппаратной реализации средств обеспечения информационной безопасности	
	1.5.3 Проверка ОИ на базе вычислительной техники на соответствие требованиям по защите информации от НСД	
	Практические занятия	**4**
	Практическое занятие №78 Работа с нормативными документами по сертификации программно-аппаратных средств	
	Практическое занятие №79 Составление отчётов по проверке объектов информатизации	
	Устный зачёт по темам 1.1 – 1.5	**2**
Самостоятельная работа		**30**
Заполнение рабочей тетради для самостоятельных работ по МДК.03.01 в СДО на платформе Moodle		30
Раздел 2 Криптографические средства защиты информации		**108**
МДК 02.02 Криптографические средства защиты информации		**108**
	Содержание учебного материала	**20**

Тема 2.1 Математические основы криптографии	2.1.1. Делимость чисел. Признаки делимости. Простые и составные числа. Проверка чисел на простоту. Алгоритмы генерации простых чисел.	
	2.1.2. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма.	
	2.1.3. Наибольший общий делитель. Применение алгоритма Евклида для нахождения НОД.	
	2.1.4 Понятие матрицы. Способы перемножения матриц.	
	Устный зачет по теме 1.	
	Практические занятия	**8**
	Практическое занятие № 1. «Проверка чисел на простоту».	
	Практическое занятие № 2. «Реализация алгоритма Евклида на языке Python».	
	Практическое занятие № 3. «Решение задач с элементами теории чисел».	
	Практическое занятие № 4. «Перемножение матриц».	
Тема 2.2 Основные термины и определения в криптографии	**Содержание учебного материала**	**6**
	2.2.1. Основные термины и определения в криптографии. Классификация основных методов криптографической защиты.	
	2.2.2. Методы симметричного шифрования. Методы ассиметричного шифрования, их применение в реальной жизни.	
	2.2.3. Основные требования, предъявляемые к криптосистемам. Принцип Киркхоффса.	
Тема 2.3 Классификация шифов	**Содержание учебного материала**	**16**
	2.3.1 Шифры замены. Шифры однозначной замены. Полиграммные шифры. Шифр Хилла.	
	2.3.2 Шифры перестановки. Шифры одинарной и множественной перестановки.	
	2.3.3 Шифры гаммирования. Генерация гаммы.	
	2.3.4 Применение генераторов ПСЧ в криптографии. Методы получения псевдослучайных последовательностей. Метод Фибоначчи.	
	2.3.5 Шифрование с открытым ключом. Алгоритм RSA.	
	2.3.6 Алгоритм на основе задачи об укладке ранца. Алгоритм на основе эллиптических кривых.	
	2.3.7 Вероятностное шифрование. Алгоритм шифрования Эль-Гамаля.	
	Устный зачет по теме 3.	
	Практические занятия	**14**
	Практическое занятие № 5. Алгоритмизация шифра Цезаря	
	Практическое занятие № 6. Комплексная работа по шифрам замены и шифрам перестановки.	
	Практическое занятие № 7. Изучение реализации классических шифров замены и перестановки в программе Cryptool (или аналоге).	
	Практическое занятие № 8. Применение шифров гаммирования.	

	Практическое занятие № 9. Изучение криптосистемы RSA.	
	Практическое занятие № 10. Реализация алгоритма RSA на языке Python.	
	Практическое занятие № 11. Использование криптосистемы Эль-Гамаля	
Тема 2.4 Основы криптоанализа	**Содержание учебного материала**	**6**
	2.4.1. Угрозы безопасности при использовании криптографии. Общие сведения о криптоанализе.	
	2.4.2. Методы криптоанализа. Частотный анализ. Метод полного перебора. Методы криптоанализа блочных шифров.	
	Устный зачет по теме 4.	
	Практические занятия	**4**
	Практическое занятие № 12. Декодирование моноалфавитного подстановочного шифра частотным методом.	
	Практическое занятие № 13. Способы защиты от атак на одноразовые пароли.	
Тема 2.5 Криптографические протоколы	**Содержание учебного материала**	**14**
	2.5.1. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана-Меркла.	
	2.5.2. Протоколы аутентификации (идентификации). Протокол проверки подлинности Kerberos	
	2.5.3. Хеш-функции. Принцип работы алгоритма хэширования MD5.	
	2.5.4. Протоколы электронной цифровой подписи. Протокол на базе алгоритма RSA. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.	
	2.5.5. Протоколы электронных платежей. Цифровые деньги. Протоколы голосования.	
	2.5.6. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана-Меркла.	
	Устный зачет по теме 5.	
	Практические занятия	**8**
	Практическое занятие № 14. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	
	Практическое занятие № 15. Использование хэш-функции.	
	Практическое занятие № 16. Реализация электронной цифровой подписи на языке Python.	
	Практическое занятие № 17. Обзор и сравнительный анализ существующего программного обеспечения для встраивания ЦВЗ.	
Тема 2.6 Кодирование информации	**Содержание учебного материала**	**2**
	2.6.1 Кодирование информации. Общедоступные кодовые системы. Секретные кодовые системы.	
	Практические занятия	**10**
	Практическое занятие № 18. Кодирование информации.	
Тема 2.7 Классическая и	**Содержание учебного материала**	
	2.7.1. Классическая стеганография. Компьютерная стеганография.	

компьютерная стеганография	2.7.2. Методы сокрытия и обнаружения информации в изображениях.	
	2.7.3. Методы сокрытия и обнаружения информации в аудиофайлах.	
	2.7.4. Методы сокрытия и обнаружения информации в видеофайлах.	
	Устный зачет по теме 7.	
	Практические работы	**6**
	Практическое занятие № 19. Анализ графических изображений на наличие скрытой информации.	
	Практическое занятие № 20. Решение ситуационных задач.	
	Практическое занятие № 21. Исследование методов стеганографии.	
Самостоятельная работа		**12**
Заполнение рабочей тетради по МДК.02.02 в СДО на платформе Moodle		**12**

Курсовая работа	**20**
Тематика курсовых работ «Организация защиты информации на предприятии» по индивидуальным вариантам	
Учебная практика	**36**
Производственная практика	**324**
Промежуточная аттестация	**18**
Всего по ПМ.02	**776**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля требует лаборатории «Технических средств защиты информации, программно-аппаратных средств защиты информации».

Оборудование кабинета информационной безопасности:

- рабочие столы и стулья по количеству обучающихся;
- компьютеры с лицензионным программным обеспечением и мультимедиапроектор, экран.

Оборудование лаборатории технических средств защиты информации:

- лаборатория программных и программно-аппаратных средств защиты информации.

Оборудование полигона подразделение защиты информации:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий, в т.ч. на электронных носителях.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением на каждом посадочном месте обучающихся и на рабочем месте преподавателя.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная литература

1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 https://e.lanbook.com/book/82817

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. https://urait.ru/bcode/449548

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. https://urait.ru/bcode/456793

4. Ложкина, Е. А. Проектирование в среде 3ds Max : учебное пособие : [16+] / Е. А. Ложкина, В. С. Ложкин ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 180 с. Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php? page=book&id=574829. Дополнительные источники 1. Компьютерное моделирование: учебник / В. М. Градов, Г. В. Овечкин, П. В. Овечкин, И. В. Рудаков. — Москва: КУРС : ИНФРА-М, 2020. — 264 с. - ISBN 978-5- 906818-79-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1062639. 2. Акопов, А. С. Компьютерное моделирование: учебник и практикум для среднего профессионального образования / А. С. Акопов. — Москва: Издательство Юрайт, 2021. — 389 с. — (Профессиональное образование). — ISBN 978-5-534-10712-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/475883.

Дополнительная литература

1. Белов В.В. Проектирование информационных систем: учебник для студ. учреждений высш. проф. образования / В. В. Белов, В. И. Чистякова; под ред. В. В. Белова – М.: Издательский центр «Академия», 2013.

2. Гвоздева В.А., Лаврентьева И.Ю., Основы построения автоматизированных информационных систем, Москва, ИД Форум – ИНФРА-М, 2009.

3. Гвоздева Т.В., Баллод Б.А., Проектирование информационных систем: учеб.пособие / Т.В. Гвоздева, Б.А. Баллод. – Ростов н/Д: Феникс, 2009. – 508 с.

4. Емельянова Н.З., Устройство и функционирование информационных систем: учеб.пособие для СПО / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – 2-е изд., перераб. и доп. – М.: Форум, 2015. – 448 с.

5. Избачков Ю.С., Информационные системы: учебник для вузов [Гриф УМО МО РФ]. 3-е изд. / Избачков Ю.С., Петров В.Н [и др.]. – СПб.: Питер, 2011. – 544 с.

6. Кугаевский С. С. Реверс-инжиниринг и быстрое прототипирование в машиностроении : учебно-методическое пособие : Рекомендовано методическим советом Уральского федерального университета для студентов вуза, обучающихся по направлениям подготовки 15.04.05 — Конструкторско-технологическое обеспечение машиностроительных производств, 09.04.01 — Информатика и вычислительная техника / С. С. Кугаевский ; научный редактор О. Г. Блинков ; Министерство науки и высшего образования Российской Федерации, Уральский федеральный университет имени первого Президента России Б. Н. Ельцина. — Екатеринбург : Издательство Уральского университета, 2023. — 98 с. — ISBN 978-5-7996-3697-5. — Текст : непосредственный.

7. Зленко М.А., Нагайцев М.В., Довбыш В.М. Аддитивные технологии в машиностроении : пособие для инженеров. М. : ГНЦ РФ ФГУП «НАМИ», 2015. 220 с. 3. Трофимов А.В. Компьютерные технологии в машиностроении. Аддитивные технологии [Электронный ресурс] : учеб. пособие. СПб. : СПбГЛТУ, 2019. 72 с. URL: https://e.lanbook.com/book/120060 (дата обращения: 28.11.2021). Доступ для авториз. Пользователей

4.3. Общие требования к организации образовательного процесса

Освоению данного модуля предшествует изучение общепрофессиональных дисциплин, таких как: основы информационной безопасности, технические средства информатизации, информатика, основы информационной безопасности.

В процессе обучения используются имитационные и информационно-коммуникационные технологии.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарным курсам: высшее педагогическое или высшее экономическое образование.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: высшее педагогическое или высшее экономическое образование.

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

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Установленные и настроенные программные и программно-аппаратные средства защиты информации	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.

Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Осуществление обработки, хранения и передачи информации ограниченного доступа.	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	Уничтожение информации с использованием программных и программно-аппаратных средств	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.
Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Журналирование действий в АС с использованием программно-аппаратных средств, средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы. Экспертная оценка разработанных материалов Наблюдения при выполнении практических работ и наблюдение в процессе практики Экзамен по ПМ.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 01. Выбирать способы решения задач профессиональ-	выбор и применение эффективных методов и способов решения профессиональных задач в профессиональной области;	Проверка качества выполнения практических работ, проверка отчетной документации по практике

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ной деятельности применительно к различным контекстам.	собственная оценка эффективности и качества выполнения заданий.	
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.	эффективный поиск необходимой информации; использование различных источников, включая электронные	Анализ результатов практических работ
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.	Эффективное планирование профессионального и личного развития	Анализ результатов практических работ
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.	взаимодействие с обучающимися, преподавателями в ходе обучения работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.	взаимодействие с обучающимися, преподавателями в ходе обучения	Анализ результатов практических работ
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.	взаимодействие с обучающимися, преподавателями в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении	работа в группах, выполнение групповых заданий	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.		
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Соблюдение режима труда и отдыха, здоровьесберегающих технологий в процессе решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.	Анализ инноваций в сфере защиты информации; работа с различными прикладными программами	Анализ результатов практических работ