**Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение**

**«Академия управления городской средой, градостроительства и печати»**

**ПРИНЯТО**

На заседании педагогического совета
протокол № 4
от 27.05.2025
Принято с учётом
согласования с
организацией –партнёром
ITСтудия «Северный ветер»
04.04.2025

**УТВЕРЖДАЮ**

Директор СПб ГБПОУ «АУГСГиП»
_____ А.М. Кривоносов

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F888BBB6190C0BBF783F46124F237295
Владелец: Кривоносов Анатолий Михайлович
Действителен: с 14.05.2025 до 07.08.2026

# РАБОЧАЯ ПРОГРАММА

**профессионального модуля**

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

**по специальности**
**10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Квалификация
**Техник по защите информации**

Санкт-Петербург
2025год

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Минобрнауки России от 09.12.2016 № 1553.

Рассмотрена на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол №3 от 16.04.2025

Разработчики: Ипатова С.В./ Оболенская Е.Г- методисты СПб ГБПОУ «АУГСГиП»

**СОДЕРЖАНИЕ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **5**

**2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **8**

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **22**

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** **28**

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

## 1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные компетенции:

1.1.1 Перечень общих компетенций

| Код | Наименование общих компетенций |
|---|---|
| ОК 1 | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. |
| ОК 2 | Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности. |
| ОК 3 | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях. |
| ОК 4 | Эффективно взаимодействовать и работать в коллективе и команде. |
| ОК 5 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста. |
| ОК 6 | 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 7 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. |
| ОК 9 | Пользоваться профессиональной документацией на государственном и иностранном языках. |

1.1.2 Перечень профессиональных компетенций

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| **ВД 2** | **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. |

1.1.3 В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| иметь практический опыт в: | – установки, настройки программных средств защиты информации в автоматизированной системе;<br>– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;<br>– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации ;<br>– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;<br>– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных;<br>– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; работы с подсистемами регистрации событий;<br>– выявления событий и инцидентов безопасности в автоматизированной системе. |
| знать: | – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;<br>– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;<br>– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;<br>– основные понятия криптографии и типовых криптографических методов и средств защиты информации;<br>– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;<br>– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. |
| уметь: | – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– устанавливать и настраивать средства антивирусной защиты в соответствии |

| | |
|---|---|
| | с предъявляемыми требованиями;<br>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;<br>– применять программные и программно-аппаратные средства для защиты информации в базах данных;<br>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;<br>– применять математический аппарат для выполнения криптографических преобразований;<br>– использовать типовые программные криптографические средства, в том числе электронную подпись;<br>– применять средства гарантированного уничтожения информации;<br>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– 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 |

1.2 Количество часов, отводимое на освоение профессионального модуля

Всего 586 часов:
из них на освоение МДК – 388 часов, в том числе на самостоятельную работу 64 ч.
на практики, в том числе учебную 108 часов и производственную 72 часа,
- экзамен по модулю 18 часов, в том числе на самостоятельную работу по подготовке 2 часов

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1. Структура профессионального модуля

| Коды профессиональных и общих компетенций | Наименования разделов профессионального модуля | Суммарный объем нагрузки, час | Объем профессионального модуля, академические часы. | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Работа обучающегося во взаимодействии с преподавателем | | | | | | | | | | | Сам.работа | |
| | | | Всего | Обучение по МДК | | | | | | Практика | | Консультации к экзамену по ПМ | Экзамен по ПМ | В период обучения по МДК | Подготовка к экзаменам |
| | | | | в том числе | | | | | | | | | | | |
| | | | | теоретические занятия | практические занятия | курсовые работы | консультации | | Экзамен по МДК | учебная | производственная | | | | |
| | | | | | | | к курсовым | к экзамену по МДК | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| ОК 01-09 ПК 2.1-2.6 | МДК 02.01 Программные и программно-аппаратные средства защиты информации | **210** | **176** | **92** | **48** | **30** | **6** | | | | | | | **34** | |
| | МДК.02.02 Криптографические средства защиты информации | **178** | **148** | **92** | **56** | | | | | | | | | **30** | |
| ОК 01-09 ПК 2.1-2.6 | **Учебная практика** | **108** | **108** | | | | | | | **108** | | | | | |
| | **Производственная практика** | **72** | **72** | | | | | | | | **72** | | | | |
| | **Экзамен по профессиональному модулю** | **18** | **16** | | | | | | | | | **4** | **12** | | **2** |
| | **Всего** | **586** | **520** | **184** | **104** | **30** | **6** | | | **108** | **72** | **4** | **12** | **64** | **2** |

**2. Тематический план и содержание профессионального модуля (ПМ.02 )**

| Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект) | Объем часов |
|---|---|---|
| 1 | 2 | 3 |
| **МДК.02.01. Программные и программно-аппаратные средства защиты информации** | | **210/5,83** |
| **Раздел 1. Основные принципы программной и программно-аппаратной защиты информации** | | |
| **Тема 1.1.** Предмет и задачи программно-аппаратной защиты информации | **Содержание** | |
| | Предмет и задачи программно-аппаратной защиты информации | 4 |
| | Основные понятия программно-аппаратной защиты информации | |
| | Классификация методов и средств программно-аппаратной защиты информации | |
| **Тема 1.2.** Стандарты безопасности | **Содержание** | |
| | Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты) | 4 |
| | Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов. | 6 |
| | Обзор стандартов. Работа с содержанием стандартов | |
| **Тема 1.3.** Защищенная автоматизированная система | **Содержание** | |
| | Автоматизация процесса обработки информации | 4 |
| | Понятие автоматизированной системы. | |
| | Особенности автоматизированных систем в защищенном исполнении. | |
| | Основные виды АС в защищенном исполнении. | |

| | | |
|---|---|---|
| | Методы создания безопасных систем | |
| | Методология проектирования гарантированно защищенных КС | |
| | Дискреционные модели | |
| | Мандатные модели | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Учет, обработка, хранение и передача информации в АИС | 6 |
| | Ограничение доступа на вход в систему. | |
| | Идентификация и аутентификация пользователей | |
| | Разграничение доступа. | |
| | Регистрация событий (аудит). | |
| | Контроль целостности данных | |
| | Уничтожение остаточной информации. | |
| | Управление политикой безопасности. Шаблоны безопасности | |
| | Криптографическая защита. Обзор программ шифрования данных | |
| | Управление политикой безопасности. Шаблоны безопасности | |
| **Тема 1.4.** Дестабилизирующее воздействие на объекты защиты | **Содержание** | |
| | Источники дестабилизирующего воздействия на объекты защиты | 4 |
| | Способы воздействия на информацию | |
| | Причины и условия дестабилизирующего воздействия на информацию | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Распределение каналов в соответствии с источниками воздействия на информацию | 4 |
| **Тема 1.5.** Принципы программно-аппаратной защиты информации от несанкционированного доступа | **Содержание** | |
| | Понятие несанкционированного доступа к информации | 6 |
| | Основные подходы к защите информации от НСД | |
| | Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам | |
| | Доступ к данным со стороны процесса | |
| | Особенности защиты данных от изменения. Шифрование. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Организация доступа к файлам | 4 |

| | | |
|---|---|---|
| | Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД | |
| **Раздел 2. Защита автономных автоматизированных систем** | | |
| **Тема 2.1.** Основы защиты автономных автоматизированных систем | **Содержание** | |
| | Работа автономной АС в защищенном режиме | 6 |
| | Алгоритм загрузки ОС. Штатные средства замыкания среды | |
| | Расширение BIOS как средство замыкания программной среды | |
| | Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка) | |
| | Применение закладок, направленных на снижение эффективности средств, замыкающих среду. | |
| **Тема 2.2.**Защита программ от изучения | **Содержание** | |
| | Изучение и обратное проектирование ПО | 6 |
| | Способы изучения ПО: статическое и динамическое изучение | |
| | Задачи защиты от изучения и способы их решения | |
| | Защита от отладки. | |
| | Защита от дизассемблирования | |
| | Защита от трассировки по прерываниям. | |
| **Тема 2.3.** Вредоносное программное обеспечение | **Содержание** | |
| | Вредоносное программное обеспечение как особый вид разрушающих воздействий | 4 |
| | Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения | |
| | Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. | |
| | Бот-неты. Принцип функционирования. Методы обнаружения | |
| | Классификация антивирусных средств. Сигнатурный и эвристический анализ | |
| | Защита от вирусов в "ручном режиме" | |
| | Основные концепции построения систем антивирусной защиты на предприятии | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО | 2 |
| **Тема 2.4.** Защита программ | **Содержание** | |

| | | |
|---|---|---|
| и данных от несанкционированного копирования | Несанкционированное копирование программ как тип НСД | 4 |
| | Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. | |
| | Привязка ПО к аппаратному окружению и носителям. | |
| | Защитные механизмы в современном программном обеспечении на примере MS Office | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Защита информации от несанкционированного копирования с использованием специализированных программных средств | 2 |
| | Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) | |
| **Тема 2.5.** Защита информации на машинных носителях | **Содержание** | |
| | Проблема защиты отчуждаемых компонентов ПЭВМ. | 6 |
| | Методы защиты информации на отчуждаемых носителях. Шифрование. | |
| | Средства восстановления остаточной информации. Создание посекторных образов НЖМД. | |
| | Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов | |
| | Безвозвратное удаление данных. Принципы и алгоритмы. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение средства восстановления остаточной информации на примере Foremost или аналога | 8 |
| | Применение специализированного программно средства для восстановления удаленных файлов | |
| | Применение программ для безвозвратного удаления данных | |
| | Применение программ для шифрования данных на съемных носителях | |
| **Тема 2.6**. Аппаратные средства идентификации и аутентификации пользователей | **Содержание** | |
| | Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ | 4 |
| | Устройства Touch Memory | |
| **Тема 2.7.** Системы обнаружения атак и вторжений | **Содержание** | |
| | СОВ и СОА, отличия в функциях. Основные архитектуры СОВ | 4 |
| | Использование сетевых снифферов в качестве СОВ | |
| | Аппаратный компонент СОВ | |
| | Программный компонент СОВ | |
| | Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений. | |

| | | |
|---|---|---|
| | **Тематика практических занятий и лабораторных работ** | |
| | Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений | 2 |
| **Раздел 3. Защита информации в локальных сетях** | | |
| **Тема 3.1.** Основы построения защищенных сетей | **Содержание** | |
| | Сети, работающие по технологии коммутации пакетов | 4 |
| | Стек протоколов TCP/IP. Особенности маршрутизации. | |
| | Штатные средства защиты информации стека протоколов TCP/IP. | |
| | Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения. | |
| **Тема 3.2.** Средства организации VPN | **Содержание** | |
| | Виртуальная частная сеть. Функции, назначение, принцип построения | 4 |
| | Криптографические и некриптографические средства организации VPN | |
| | Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. | |
| | Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки | |
| | Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Развертывание VPN | 2 |
| **Раздел 4. Защита информации в сетях общего доступа** | | |
| **Тема 4.1.**Обеспечение безопасности межсетевого взаимодействия | **Содержание** | |
| | Методы защиты информации при работе в сетях общего доступа. | 6 |
| | Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности | |
| | Основные типы firewall. Симметричные и несимметричные firewall. | |
| | Уровень 1. Пакетные фильтры | |
| | Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. | |
| | Уровень 3. Proxy-сервера прикладного уровня | |
| | Однохостовые и мультихостовые firewall. | |
| | Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций | |
| | Требования по сертификации межсетевых экранов | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. | 4 |

| | | |
|---|---|---|
| | Изучение различных способов закрытия "опасных" портов | |
| **Раздел 5. Защита информации в базах данных** | | |
| **Тема 5.1.** Защита информации в базах данных | **Содержание** | |
| | Основные типы угроз. Модель нарушителя | 6 |
| | Средства идентификации и аутентификации. Управление доступом | |
| | Средства контроля целостности информации в базах данных | |
| | Средства аудита и контроля безопасности. Критерии защищенности баз данных | |
| | Применение криптографических средств защиты информации в базах данных | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Изучение механизмов защиты СУБД MS Access | 4 |
| | Изучение штатных средств защиты СУБД MSSQL Server | |
| **Раздел 6. Мониторинг систем защиты** | | |
| **Тема 6.1.** Мониторинг систем защиты | **Содержание** | |
| | Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации | 6 |
| | Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25 | |
| | Классификация отслеживаемых событий. Особенности построения систем мониторинга | |
| | Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. | |
| | Классификация сетевых мониторов | |
| | Системы управления событиями информационной безопасности (SIEM).<br>Обзор SIEM-систем на мировом и российском рынке. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов | 2 |
| | Проведение аудита ЛВС сетевым сканером | |
| **Тема 6.2.** Изучение мер защиты информации в информационных системах | **Содержание** | |
| | Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты. | 2 |
| | **Тематика практических занятий и лабораторных работ** | |

| | | |
|---|---|---|
| | Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке. | 2 |
| **Тема 6.3.** Изучение современных программно-аппаратных комплексов. | **Содержание** | |
| | Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов | 6 |
| | Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов | |
| | Изучение типовых решений для построения VPN на примере VipNet или других аналогов | |
| | Изучение современных систем антивирусной защиты на примере корпоративных решений Kaspersky-Lab или других аналогов | |
| | Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов | |
| **Курсовая работа** | | **30** |
| **Примерная тематика курсовых работ**<br>1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)<br>2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)<br>3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание)<br>4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание)<br>5. Проблема защиты информации в облачных хранилищах данных и ЦОДах<br>6. Защита сред виртуализации | | |
| **Консультации к курсовому проекту**<br>Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования. | | **6** |
| **Дифференцированный зачёт** | | **2** |
| Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)<br>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, | | **34** |

| | | |
|---|---|---|
| отчетов к их защите.<br>**Тематика самостоятельной работы при изучении МДК.02.01**<br>1. Изучение новых технологий хранения информации<br>2. Статистика и анализ крупных утечек информации за год<br>3. Поиск информации о новых видах атак на информационную систему<br>4. Обзор современных программных и программно-аппаратных средств защиты<br>5. Сравнительный анализ современных программных и программно-аппаратных средств защиты | | |
| **МДК.02.02 Криптографические средства защиты информации** | | **178/4,94** |
| **Введение** | **Содержание** | |
| | Предмет и задачи криптографии. История криптографии. Основные термины | 2 |
| **Раздел 1. Математические основы защиты информации** | | |
| **Тема 1.1.** Математические основы криптографии | **Содержание** | |
| | Элементы теории множеств. Группы, кольца, поля. | 24 |
| | Делимость чисел. Признаки делимости. Простые и составные числа. | |
| | Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД. | |
| | Отношения сравнимости. Свойства сравнений. Модулярная арифметика. | |
| | Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю. | |
| | Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. | |
| | Китайская теорема об остатках. | |
| | Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена. | |
| | Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда. | |
| | Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра. | |
| | Арифметические операции над большими числами. | |
| | Эллиптические кривые и их приложения в криптографии. | |
| | **Тематика практических занятий и лабораторных работ** | |

| | | |
|---|---|---|
| | Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений | 4 |
| | Проверка чисел на простоту | |
| | Решение задач с элементами теории чисел. | |
| **Раздел 2. Классическая криптография** | | |
| **Тема 2.1.** Методы криптографического защиты информации | **Содержание** | |
| | Классификация основных методов криптографической защиты. Методы симметричного шифрования | 8 |
| | Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр | |
| | Методы перестановки. Табличная перестановка, маршрутная перестановка | |
| | Гаммирование. Гаммирование с конечной и бесконечной гаммами | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение классических шифров замены | 4 |
| | Применение классических шифров перестановки | |
| | Применение метода гаммирования | |
| **Тема 2.2.** Криптоанализ | **Содержание** | |
| | Основные методы криптоанализа. Криптографические атаки. | 8 |
| | Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса | |
| | Перспективные направления криптоанализа, квантовый криптоанализ. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Криптоанализ шифра простой замены методом анализа частотности символов | 8 |
| | Криптоанализ классических шифров методом полного перебора ключей | |
| | Криптоанализ шифра Вижинера | |
| **Тема 2.3.** Поточные шифры и генераторы псевдослучайных чисел | **Содержание учебного материала** | |
| | Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии | 6 |
| | Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение методов генерации ПСЧ | 2 |
| **Раздел 3. Современная криптография** | | |
| **Тема 3.1.** Кодирование ин- | **Содержание учебного материала** | |

| | | |
|---|---|---|
| формации. Компьютеризация шифрования. | Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII | 6 |
| | Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Кодирование информации | 8 |
| | Программная реализация классических шифров | |
| | Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге. | |
| **Тема 3.2.** Симметричные системы шифрования | **Содержание учебного материала** | |
| | Общие сведения. Структурная схема симметричных криптографических систем | 4 |
| | Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4 | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Изучение программной реализации современных симметричных шифров | 4 |
| **Тема 3.3.** Асимметричные системы шифрования | **Содержание учебного материала** | |
| | Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. | 6 |
| | Элементы теории чисел в криптографии с открытым ключом. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение различных асимметричных алгоритмов. | 4 |
| | Изучение программной реализации асимметричного алгоритма RSA | |
| **Тема 3.4.** Аутентификация данных. Электронная подпись | **Содержание учебного материала** | |
| | Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи | 4 |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение различных функций хеширования, анализ особенностей хешей | 8 |
| | Применение криптографических атак на хеш-функции. | |

| | | |
|---|---|---|
| | Изучение программно-аппаратных средств, реализующих основные функции ЭП | |
| **Тема 3.5.** Алгоритмы обмена ключей и протоколы аутентификации | **Содержание учебного материала** | |
| | Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация | 4 |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение протокола Диффи-Хеллмана для обмена ключами шифрования. | 6 |
| | Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos. | |
| **Тема 3.6.** Криптозащита информации в сетях передачи данных | **Содержание учебного материала** | |
| | Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр | 6 |
| | Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP. | |
| **Тема 3.7.** Защита информации в электронных платежных системах | **Содержание учебного материала** | |
| | Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер | 6 |
| | Применение криптографических протоколов для обеспечения безопасности электронной коммерции. | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей | 4 |
| **Тема 3.8.** Компьютерная стеганография | **Содержание учебного материала** | |
| | Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. | 6 |
| | Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ | |
| | **Тематика практических занятий и лабораторных работ** | |
| | Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ | 4 |
| | Реализация простейших стеганографических алгоритмов | |
| | **Дифференцированный зачёт** | 2 |

| | |
|---|---|
| Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)<br>Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.<br>**Тематика самостоятельной работы при изучении МДК.02.02**<br>1. История развития криптографии<br>2. Программная реализация классических шифров<br>3. Оптимизация методов частотного анализа моноалфавитных шифров.<br>4. Программная реализация классических шифров<br>5. Методы механизации шифрования<br>6. Цифровое представление различных форм информации<br>7. Анализ современных симметричных криптоалгоритмов<br>8. Анализ современных асимметричных криптоалгоритмов<br>9. Программная реализация современных криптоалгоритмов<br>10. Сравнительный анализ функций хеширования<br>11. Аутентификация сообщений<br>12. Законодательство в области криптографической защиты информации<br>13. Перспективные направления криптографии | **30** |
| **Учебная практика**<br>**Виды работ:**<br>– Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах<br>– Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности<br>– Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности<br>– Составление документации по учету, обработке, хранению и передаче конфиденциальной информации<br>– Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации<br>– Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.<br>– Устранение замечаний по результатам проверки | **108** |

| | |
|---|---|
| – Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.<br>– Применение математических методов для оценки качества и выбора наилучшего программного средства<br>– Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи | |
| **Производственная практика по ПМ.02**<br>**Виды работ**<br>– Анализ принципов построения систем информационной защиты производственных подразделений.<br>– Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.<br>– Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;<br>– Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении<br>– Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации<br>– Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | **72** |
| **Экзамен по модулю** | **12** |
| **Консультации к экзамену по модулю** | **4** |
| **Самостоятельная работа по подготовке к экзамену по модулю** | **2** |
| **Всего по ПМ.01** | ***586/16,28*** |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 30, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

Оборудование лаборатории «Программных и программно-аппаратных средств обеспечения информационной безопасности» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- рабочее место преподавателя;
- учебно-методическое обеспечение модуля;
- интерактивная доска, комплект презентаций;
- антивирусные программные комплексы;
- программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;
- программные и программно-аппаратные средства обнаружения атак (вторжений), поиска уязвимостей;
- средства уничтожения остаточной информации в запоминающих устройствах;
- программные средства криптографической защиты информации.

Реализация программы профессионального обучения предполагает обязательную Учебную/производственную практики. Учебная практика реализуется в лабораториях академии и оснащена оборудованием, инструментами, расходными материалами, обеспечивающих выполнение всех видов работ.

Технологическое оснащение рабочих мест учебной практики соответствует содержанию профессиональной деятельности и даёт возможность обучающемуся овладеть знаниями, умениями и навыками по всем видам деятельности, предусмотренных программой, с использованием современных технологий, материалов и оборудования.

**3.2. Информационное обеспечение обучения**

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендованные ФУМО, для использования в образовательном процессе.

**Основные источники:**

1. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учеб. Пособие. – М.: Горячая линия – Телеком, 2017.- 175 с.

2. Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – М.:

Горячая линия – Телеком, 2016.- 248 с.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

5. 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

6. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

7. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии (учебное пособие). - М.: Гелиос АРВ, 2005. – гриф Министерства образования РФ по группе специальностей в области информационной безопасности

8. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

9. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

10. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

**Дополнительные источники:**

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006. Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г

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

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

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

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

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

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

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

9. 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».

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

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

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

13. 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.

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

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

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

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.

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

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

20. 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.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

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 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

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

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

39. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

40. 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.

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

42. 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.

43. 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.

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

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

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

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

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

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

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

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

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

**Периодические издания:**

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

**Электронные источники:**

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. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| **Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля** | **Критерии оценки** | **Методы оценки** |
|---|---|---|
| ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. | Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации | Текущий контроль в форме:<br>устных зачетов по темам;<br>оценки выполнения практических работ;<br>оценки выполнения самостоятельной работы.<br>Выполнении работ по учебной и производственной практикам<br>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы<br>Экзамен по ПМ. |
| ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. | Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | |
| ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. | Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации | |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. | Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа | |
| ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. | Демонстрация алгоритма проведения работ по уничтожению информации и носителей 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, пре- | Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак | |

| | | |
|---|---|---|
| дупреждения и ликвидации последствий компьютерных атак. | | |
| ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | – обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;<br>– адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | 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 | – оперативность поиска и использования информации, необходимой для качественного выполнения профессиональных задач,<br>– широта использования различных источников информации, включая электронные | 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 финансовой грамотности в различных жизненных ситуациях | -демонстрация ответственности за принятые решения;<br>– обоснованность самоанализа и коррекция результатов собственной работы | ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях |
| ОК04 Эффективно взаимодействовать и работать в коллективе и команде | –конструктивность взаимодействия с обучающимися, преподавателями и руководителями практики в ходе обучения и при решении профессиональных задач;<br>– четкое выполнение обязанностей при работе в команде и/или выполнении задания в группе;<br>– соблюдение норм профессиональной этики при работе в команде;<br>– построение профессионального общения с учетом социально-профессионального статуса, | ОК04 Эффективно взаимодействовать и работать в коллективе и команде |

| | | |
|---|---|---|
| | ситуации общения, особенностей группы и индивидуальных особенностей участников коммуникации | |
| ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | – грамотность устной и письменной речи,<br>– ясность формулирования и изложения мыслей<br>– проявление толерантности в рабочем коллективе | 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. | описывать значимость своей специальности для развития экономики и среды жизнедеятельности граждан российского государства; | ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих 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 | – соблюдать нормы экологической безопасности;<br>– применение направлений ресурсосбережения в рамках профессиональной деятельности по специальности<br>- применять в работе принципы бережливого производства, анализировать процесс работы на предмет выявления потерь и для совершенствования процесса<br>- уметь действовать и знать алгоритм действий при возникновении чрезвычайных ситуаций | 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 фи- | - выполнять действия в рабочем процессе с учетом эргономики и с учетом безопасности движений<br>- поддерживать необходимый уровень физической подготовки | ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физиче- |

| | | |
|---|---|---|
| зической подготовленности | | ской подготовленности |
| ОК 09 Пользоваться профессиональной документацией на государственном и иностранных языках | – использование в профессиональной деятельности необходимой технической документации, в том числе на иностранных языках<br>- Понимает тексты на базовые профессиональные темы;<br>строить простые высказывания о себе и о своей профессиональной деятельности;<br>кратко обосновывать и объяснять свои действия (текущие и планируемые); | ОК 09 Пользоваться профессиональной документацией на государственном и иностранных языках |

Планируемые личностные результаты в ходе реализации программы профессионального модуля

**Личностные результаты реализации программы воспитания(для рабочих программ дисциплин /модулей)**

| **Личностные результаты реализации программы воспитания** *(дескрипторы)* | **Код личностных результатов реализации программы воспитания** |
|---|---|
| Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа» | **ЛР 4** |
| Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, народу, малой родине, знания его истории и культуры, принятие традиционных ценностей многонационального народа России. Выражающий свою этнокультурную идентичность, сознающий себя патриотом народа России, деятельно выражающий чувство причастности к многонациональному народу России, к Российскому Отечеству. Проявляющий ценностное отношение к историческому и культурному наследию народов России, к национальным символам, праздникам, памятникам, традициям народов, проживающих в России, к соотечественникам за рубежом, поддерживающий их заинтересован- | **ЛР 5** |

| | |
|---|---|
| ность в сохранении общероссийской культурной идентичности, уважающий их права | |
| Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого выбора, самоопределения.<br>Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный в отношении выражения прав и законных интересов других людей | **ЛР 7** |
| Бережливо относящийся к природному наследию страны и мира, проявляющий сформированность экологической культуры на основе понимания влияния социальных, экономических и профессионально-производственных процессов на окружающую среду. Выражающий деятельное неприятие действий, приносящих вред природе, распознающий опасности среды обитания, предупреждающий рискованное поведение других граждан, популяризирующий способы сохранения памятников природы страны, региона, территории, поселения, включенный в общественные инициативы, направленные на заботу о них | **ЛР 10** |
| Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры. Критически оценивающий и деятельно проявляющий понимание эмоционального воздействия искусства, его влияния на душевное состояние и поведение людей. Бережливо относящийся к культуре как средству коммуникации и самовыражения в обществе, выражающий сопричастность к нравственным нормам, традициям в искусстве. Ориентированный на собственное самовыражение в разных видах искусства, художественном творчестве с учётом российских традиционных духовно-нравственных ценностей, эстетическом обустройстве собственного быта. Разделяющий ценности отечественного и мирового художественного наследия, роли народных традиций и народного творчества в искусстве. Выражающий ценностное отношение к технической и промышленной эстетике | **ЛР 11** |
| **Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности** | |
| Способный при взаимодействии с другими людьми достигать поставленных целей, стремящийся к формированию в строительной отрасли и системе жилищно-коммунального хозяйства личностного роста как профессионала | **ЛР13** |
| Способный ставить перед собой цели под для решения возникающих профессиональных задач, подбирать способы решения и средства развития, в том числе с использованием информационных технологий; | **ЛР14** |
| Содействующий формированию положительного образа и поддержанию престижа своей профессии | **ЛР15** |
| Способный искать и находить необходимую информацию используя разнообразные технологии ее поиска, для решения возникающих в процессе производственной деятельности; | **ЛР 16** |
| Способный выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов; позиционирующий себя в се- | **ЛР 17** |

| | |
|---|---|
| ти как результативный и привлекательный участник трудовых отношений. | |