государственное автономное учреждение
Калининградской области
профессиональная образовательная организация
**«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА»**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7AD4EF0E26F9347F58545EB00C15B31C
Владелец: ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ КАЛИНИНГРАДСКОЙ ОБЛАСТИ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ "КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА"
Действителен: с 07.11.2022 до 31.01.2024

# РАБОЧАЯ ПРОГРАММА ПРОФЕССИАОНАЛЬНОГО МОДУЛЯ

## Защита информации в автоматизированных системах программными и программно-аппаратными средствами

**2023**

СОГЛАСОВАНО
Заместитель директора по УМР
ГАУ КО «Колледж предпринимательства»

_____ Ю.И. Бурыкина

30 июня 2023 года

УТВЕРЖДАЮ
Директор ГАУ КО
«Колледж предпринимательства»

_____ Л.Н. Копцева

30 июня 2023 года

Рабочая программа профессионального модуля разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО) по специальности **10.02.05 Обеспечение безопасности информационных систем.**

Организация-разработчик: государственное автономное учреждение Калининградской области профессиональная образовательная организация «Колледж предпринимательства»

Разработчики:
Зверев М.В. – ГАУ КО «Колледж предпринимательства», заведующий отделением
Бычай А.П. - ГАУ КО «Колледж предпринимательства», преподаватель

Рабочая программа профессионального модуля рассмотрена на заседании отделения информационных технологий. Протокол № 6 от 30.06.2022 г.

**СОДЕРЖАНИЕ**

# 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

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

| 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. |

### 1.1.2. Общие компетенции:

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ОК 01. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 02. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 03. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 04. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 05. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 06. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. |
| ОК 07. | Содействовать сохранению окружающей среды, ресурсосбережению, 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. | Использовать информационные технологии в профессиональной деятельности. |

| | |
|---|---|
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |
| ОК 11. | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. |

## 1.1.3. В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| **Иметь практический опыт** | – 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;<br>– работы с подсистемами регистрации событий;<br>– выявления событий и инцидентов безопасности в автоматизированной системе. |
| **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; |

| | |
|---|---|
| | – 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;<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. |

## 1.2. Количество часов, отводимое на освоение профессионального модуля

Всего – 724 часов, в том числе:
на освоение МДК – 460 часов;
учебной практики – 108 часов;
производственной практики – 144 часов;
экзамен по профессиональному модулю – 12 часов.

# 2.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 2.1. Структура профессионального модуля

| Коды профессиональных компетенций | Наименования разделов профессионального модуля | Объем образовательной программы, час. | Объём профессионального модуля, час | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Обучение по МДК | | | Практики | | Самостоятельная работа |
| | | | Всего, часов | лабораторные работы и практические занятия | курсовая работа (проект), часов | Учебная практика, часов | Производственная практика, часов | |
| **ПК 1.2, ПК 2.1 - ПК 2.3, ПК 2.5, ПК 2.6, ОК 1– ОК 10** | **Раздел 1 модуля.** Применение программных и программно-аппаратных средств защиты информации | **262** | **234** | 124 | 0 | 0 | 0 | 16 |
| **ПК 2.1- ПК 2.4, ПК 2.6, ОК 1– ОК 10** | **Раздел 2 модуля.** Применение криптографических средств защиты информации | **198** | **186** | 100 | 0 | 0 | 0 | 12 |
| | **Учебная практика** | **108** | | | | **108** | | |
| | **Производственная практика** | **144** | | | | | **144** | |
| | **Экзамен по профессиональному модулю** | **12** | | | | | | |
| | **Всего:** | **724** | **420** | 224 | 0 | **108** | **144** | **28** |

## 2.2. Содержание профессионального модуля Защита информации в автоматизированных системах программными и программно-аппаратными средствами

| Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) | Объем часов | Осваиваемые компетенции |
|---|---|---|---|
| **Раздел 1 модуля. Применение программных и программно-аппаратных средств защиты информации** | | **262** | |
| **МДК.02.01. Программные и программно-аппаратные средства защиты информации** | | **262** | |
| **Раздел 1. Основные принципы программной и программно-аппаратной защиты информации** | | | |
| **Тема 1.1.** Предмет и задачи программно-аппаратной защиты информации | **Содержание** | **6** | ПК 1.1. ОК 1– ОК 10 |
| | Предмет и задачи программно-аппаратной защиты информации | 2 | |
| | Основные понятия программно-аппаратной защиты информации | 2 | |
| | Классификация методов и средств программно-аппаратной защиты информации | 2 | |
| **Тема 1.2.** Стандарты безопасности | **Содержание** | **8** | ПК 1.1. ОК 1– ОК 10 |
| | Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | 2 | |
| | Профили защиты программных и программно-аппаратных средств межсетевых экранов, средств контроля съемных машинных носителей информации. | 2 | |
| | Профили защиты программных и программно-аппаратных средств доверенной загрузки, средств антивирусной защиты | 2 | |
| | Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | 2 | |
| | **Практическая работа** | **8** | |
| | Обзор нормативных правовых актов, по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | 2 | |
| | Обзор нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. | 2 | |
| | Работа с содержанием нормативных правовых актов. | 2 | |

| | | | |
|---|---|---|---|
| | Обзор стандартов. Работа с содержанием стандартов | 2 | |
| **Тема 1.3**. Защищенная автоматизированная система | **Содержание** | **16** | ПК 1.1. ОК 1– ОК 10 |
| | Автоматизация процесса обработки информации | 2 | |
| | Понятие автоматизированной системы. | 2 | |
| | Особенности автоматизированных систем в защищенном исполнении. | 2 | |
| | Основные виды АС в защищенном исполнении. | 2 | |
| | Методы создания безопасных систем | 2 | |
| | Методология проектирования гарантированно защищенных КС | 2 | |
| | Дискреционные модели | 2 | |
| | Мандатные модели | 2 | |
| | **Практическая работа** | **20** | |
| | Учет, обработка, хранение и передача информации в АИС | 2 | |
| | Ограничение доступа на вход в систему. | 2 | |
| | Идентификация и аутентификация пользователей | 2 | |
| | Разграничение доступа. | 2 | |
| | Регистрация событий (аудит). | 2 | |
| | Контроль целостности данных | 2 | |
| | Уничтожение остаточной информации. | 2 | |
| | Управление политикой безопасности. Шаблоны безопасности | 2 | |
| | Криптографическая защита. Обзор программ шифрования данных | 2 | |
| | Управление политикой безопасности. Шаблоны безопасности | 2 | |
| **Тема 1.4.** Дестабилизирующее воздействие на объекты защиты | **Содержание** | **6** | ПК 1.1. ОК 1– ОК 10 |
| | Источники дестабилизирующего воздействия на объекты защиты | 2 | |
| | Способы воздействия на информацию | 2 | |
| | Причины и условия дестабилизирующего воздействия на информацию | 2 | |
| | **Практическая работа** | **8** | |
| | Распределение каналов в соответствии с источниками воздействия на информацию | 2 | |
| | Изучение источников дестабилизирующего воздействия на объекты защиты | 2 | |
| | Изучение способов воздействия на информацию | 2 | |
| | Изучение причин и условий дестабилизирующего воздействия на информацию | 2 | |
| **Тема 1.5.** Принципы программно-аппаратной защиты информации от | **Содержание** | **10** | ПК 1.1. ОК 1– ОК 10 |
| | Понятие несанкционированного доступа к информации | 2 | |
| | Основные подходы к защите информации от НСД | 2 | |

| | | | |
|---|---|---|---|
| несанкционированного доступа | Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам | 2 | |
| | Доступ к данным со стороны процесса | 2 | |
| | Особенности защиты данных от изменения. Шифрование. | 2 | |
| | **Практическая работа** | **6** | |
| | Организация доступа к файлам | 2 | |
| | Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД | 2 | |
| | Изучение алгоритмов шифрования | 2 | |
| **Раздел 2. Защита автономных автоматизированных систем** | | | |
| **Тема 2.1.** Основы защиты автономных автоматизированных систем | **Содержание** | **10** | ПК 1.1. ОК 1– ОК 10 |
| | Работа автономной АС в защищенном режиме | 2 | |
| | Алгоритм загрузки ОС. Штатные средства замыкания среды | 2 | |
| | Расширение BIOS как средство замыкания программной среды | 2 | |
| | Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка) | 2 | |
| | Применение закладок, направленных на снижение эффективности средств, замыкающих среду. | 2 | |
| **Тема 2.2.** Защита программ от изучения | **Содержание** | **6** | ПК 1.1. ОК 1– ОК 10 |
| | Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение | 2 | |
| | Задачи защиты от изучения и способы их решения. Защита от отладки. | 2 | |
| | Защита от дизассемблирования. Защита от трассировки по прерываниям. | 2 | |
| **Тема 2.3.** Вредоносное программное обеспечение | **Содержание** | **4** | ПК 1.1. ОК 1– ОК 10 |
| | Вредоносное программное обеспечение как особый вид разрушающих воздействий. 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. | 2 | |
| | 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 | 2 | |
| | **Практическая работа** | **2** | |
| | Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО | 2 | |

| | | | |
|---|---|---|---|
| **Тема 2.4.** Защита программ и данных от несанкционированного копирования | **Содержание** | **4** | ПК 1.1. ОК 1– ОК 10 |
| | Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты от копирования. | 2 | |
| | Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office | 2 | |
| | **Практическая работа** | **6** | |
| | Защита информации от несанкционированного копирования с использованием специализированных программных средств | 2 | |
| | Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) | 2 | |
| | Привязка ПО к аппаратному окружению и носителям. | 2 | |
| **Тема 2.5.** Защита информации на машинных носителях | **Содержание** | **6** | ПК 1.1. ОК 1– ОК 10 |
| | Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Средства восстановления остаточной информации. Создание посекторных образов НЖМД.Шифрование. | 2 | |
| | Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов | 2 | |
| | Безвозвратное удаление данных. Принципы и алгоритмы. | 2 | |
| | **Практическая работа** | **10** | |
| | Применение средства восстановления остаточной информации на примере Foremost или аналога | 2 | |
| | Применение специализированного программно средства для восстановления удаленных файлов | 2 | |
| | Применение программ для безвозвратного удаления данных | 2 | |
| | Применение программ для шифрования данных на съемных носителях | 2 | |
| | Документирование результатов | 2 | |
| **Тема 2.6.** Аппаратные средства идентификации и аутентификации пользователей | **Содержание** | **4** | ПК 1.1. ОК 1– ОК 10 |
| | Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ | 2 | |
| | Устройства Touch Memory | 2 | |
| **Тема 2.7.** Системы обнаружения атак и вторжений | **Содержание** | **4** | ПК 1.1. ОК 1– ОК 10 |
| | СОВ и СОА, отличия в функциях. Основные архитектуры СОВ. Использование сетевых снифферов в качестве СОВ. Аппаратный компонент СОВ. Программный компонент СОВ | 2 | |

| | | | |
|---|---|---|---|
| | Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений. | 2 | |
| | **Практическая работа** | **6** | |
| | Моделирование проведения атаки. | 2 | |
| | Изучение инструментальных средств обнаружения вторжений | 2 | |
| | Обнаружение сигнатур. | 2 | |
| **Раздел 3. Защита информации в локальных сетях** | | | |
| **Тема 3.1.** Основы построения защищенных сетей | **Содержание** | **4** | ПК 1.1. ОК 1– ОК 10 |
| | Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. | 2 | |
| | Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения. | 2 | |
| **Тема 3.2.** Средства организации VPN | **Содержание** | **4** | ПК 1.1. ОК 1– ОК 10 |
| | Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. | 2 | |
| | Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки. Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки | 2 | |
| | **Практическая работа** | **8** | |
| | Развертывание VPN | 8 | |
| **Раздел 4. Защита информации в сетях общего доступа** | | | |
| **Тема 4.1.** Обеспечение безопасности межсетевого взаимодействия | **Содержание** | **8** | ПК 1.1. ОК 1– ОК 10 |
| | Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности. Основные типы firewall. Симметричные и несимметричные firewall. | 2 | |
| | Уровень 1. Пакетные фильтры. Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня | 2 | |
| | Однохостовые и мультихостовые firewall. | 2 | |
| | Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций. Требования по сертификации межсетевых экранов | 2 | |
| | **Практическая работа** | **10** | |
| | Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr. | 2 | |
| | Изучение различных способов закрытия "опасных" портов | 2 | |

| | | | |
|---|---|---|---|
| | Изучение методов защиты информации при работе в сетях общего доступа. | 2 | |
| | Базовая настройка межсетевого экраны типа firewall | 2 | |
| | Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. | 2 | |
| **Раздел 5. Защита информации в базах данных** | | | |
| **Тема 5.1**. Защита информации в базах данных | **Содержание** | **6** | ПК 1.1. ОК 1– ОК 10 |
| | Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом. | 2 | |
| | Средства контроля целостности информации в базах данных. Средства аудита и контроля безопасности. Критерии защищенности баз данных. | 2 | |
| | Применение криптографических средств защиты информации в базах данных. | 2 | |
| | **Практическая работа** | **8** | |
| | Изучение механизмов защиты СУБД MS Access | 4 | |
| | Изучение штатных средств защиты СУБД MSSQL Server | 4 | |
| **Раздел 6. Мониторинг систем защиты** | | | |
| **Тема 6.1.** Мониторинг систем защиты | **Содержание** | **6** | |
| | Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25 | 2 | ПК 1.1. ОК 1– ОК 10 |
| | Классификация отслеживаемых событий. Особенности построения систем мониторинга. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. | 2 | |
| | Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке. | 2 | |
| | **Практическая работа** | **8** | |
| | Изучение и сравнительный анализ распространенных сетевых мониторов на примере RealSecure, SNORT, NFR или других аналогов | 2 | |
| | Проведение аудита ЛВС сетевым сканером | 2 | |
| | Проверка ресурсов общего пользования. | 2 | |
| | Диагностика кабельного хозяйства. | 2 | |
| **Тема 6.2.** Изучение мер защиты информации в информационных системах | **Содержание** | **2** | ПК 1.1. ОК 1– ОК 10 |
| | Изучение требований о защите информации, не составляющей государственную тайну. Изучение методических документов ФСТЭК по применению мер защиты. | 2 | |
| | **Практическая работа** | **6** | |

| | | | |
|---|---|---|---|
| | Выбор мер защиты информации для их реализации в информационной системе. | 2 | |
| | Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке. | 2 | |
| | Изучение требований о защите информации. | 2 | |
| **Тема 6.3.** Изучение современных программно-аппаратных комплексов. | **Практическая работа** | **10** | ПК 1.1. ОК 1– ОК 10 |
| | Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов | 2 | |
| | Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов | 2 | |
| | Изучение типовых решений для построения VPN на примере VipNet или других аналогов | 2 | |
| | Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов | 2 | |
| | Изучение функционала и областей применения DLP систем на примере InfoWatchTrafficMonitor или других аналогов | 2 | |
| **Самостоятельная работа при изучении МДК.02.01** | | **20** | |
| Изучение новых технологий хранения информации | | | |
| Статистика и анализ крупных утечек информации за год | | | |
| Поиск информации о новых видах атак на информационную систему | | | |
| Обзор современных программных и программно-аппаратных средств защиты | | | |
| Сравнительный анализ современных программных и программно-аппаратных средств защиты | | | |
| **Промежуточная аттестация по МДК.02.01 – экзамен** | | **12** | |
| **Раздел 2 модуля. Применение криптографических средств защиты информации** | | **198** | |
| **МДК.02.02. Криптографические средства защиты информации** | | **198** | |
| **Введение** | **Содержание** | **2** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Предмет и задачи криптографии. История криптографии. Основные термины | 2 | |
| **Раздел 1. Математические основы защиты информации** | | | |
| **Тема 1.1.** Математические основы криптографии | **Содержание** | **24** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Элементы теории множеств. Группы, кольца, поля. | 2 | |
| | Делимость чисел. Признаки делимости. Простые и составные числа. | 2 | |
| | Основная теорема арифметики. Наибольший общий делитель. Взаимно | 2 | |
| | простые числа. Алгоритм Евклида для нахождения НОД. | 2 | |

| | | | |
|---|---|---|---|
| | Отношения сравнимости. Свойства сравнений. Модулярная арифметика. | 2 | |
| | Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера. Алгоритм быстрого возведения в степень по модулю. | 2 | |
| | Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. | 2 | |
| | Китайская теорема об остатках. | 2 | |
| | Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена. | 2 | |
| | Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда. | 2 | |
| | Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра. | 2 | |
| | Арифметические операции над большими числами. Эллиптические кривые и их приложения в криптографии. | 2 | |
| | **Практическая работа** | **8** | |
| | Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений | 2 | |
| | Проверка чисел на простоту | 2 | |
| | Решение задач с элементами теории чисел. | 2 | |
| | Разложение числа на множители. | 2 | |
| **Раздел 2. Классическая криптография** | | | |
| **Тема 2.1.** Методы криптографического защиты информации | **Содержание** | **8** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Классификация основных методов криптографической защиты. Методы симметричного шифрования | 2 | |
| | Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр | 2 | |
| | Методы перестановки. Табличная перестановка, маршрутная перестановка | 2 | |
| | Гаммирование. Гаммирование с конечной и бесконечной гаммами | 2 | |
| | **Практическая работа** | **8** | |
| | Применение классических шифров замены | 2 | |
| | Применение классических шифров перестановки | 2 | |
| | Применение метода гаммирования | 2 | |
| | Применение метода табличной перестановки. | 2 | |
| **Тема 2.2.** Криптоанализ | **Содержание** | **6** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Основные методы криптоанализа. Криптографические атаки. | 2 | |
| | Криптогафическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффса | 2 | |
| | Перспективные направления криптоанализа, квантовый криптоанализ. | 2 | |

| | | | |
|---|---|---|---|
| | **Практическая работа** | **10** | |
| | Криптоанализ шифра простой замены методом анализа частотности символов | 2 | |
| | Криптоанализ классических шифров методом полного перебора ключей | 2 | |
| | Криптоанализ шифра Вижинера | 2 | |
| | Изучение принципов Киркхоффса | 2 | |
| | Изучение криптографических атак. | 2 | |
| **Тема 2.3.** Поточные шифры и генераторы псевдослучайных чисел | **Содержание** | **4** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии | 2 | |
| | Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS. | 2 | |
| | **Практическая работа** | **4** | |
| | Применение методов генерации ПСЧ | 4 | |
| **Раздел 3. Современная криптография** | | | |
| **Тема 3.1.** Кодирование информации. Компьютеризация шифрования. | **Содержание** | **10** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Кодирование информации. Символьное кодирование. Смысловое кодирование. | 2 | |
| | Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII | 2 | |
| | Компьютеризация шифрования. Аппаратное и программное шифрование. | 2 | |
| | Стандартизация программно-аппаратных криптографических систем и средств. | 2 | |
| | Современные программные и аппаратные криптографические средства. | 2 | |
| | **Практическая работа** | **10** | |
| | Кодирование информации | 2 | |
| | Программная реализация классических шифров | 2 | |
| | Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге. | 2 | |
| | Изучение аппаратного и программного шифрования | 2 | |
| | Изучение современных программных и аппаратных криптографических средств. | 2 | |
| **Тема 3.2.** Симметричные системы шифрования | **Содержание** | **6** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Общие сведения. Структурная схема симметричных криптографических систем | 2 | |
| | Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. | 2 | |
| | Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4 | 2 | |
| | **Практическая работа** | **8** | |
| | Изучение программной реализации современных симметричных шифров | 8 | |
| | **Содержание** | **4** | ПК 1.2. |

| | | | |
|---|---|---|---|
| **Тема 3.3.** Асимметричные системы шифрования | Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. | 2 | ПК 1.3<br>ПК 1.4<br>ОК 1– ОК 10 |
| | Элементы теории чисел в криптографии с открытым ключом. | 2 | |
| | **Практическая работа** | **8** | |
| | Применение различных асимметричных алгоритмов. | 4 | |
| | Изучение программной реализации асимметричного алгоритма RSA | 4 | |
| **Тема 3.4.** Аутентификация данных. Электронная подпись | **Содержание** | **4** | ПК 1.2.<br>ПК 1.3<br>ПК 1.4<br>ОК 1– ОК 10 |
| | Аутентификация данных. Общие понятия. ЭП. МАС. | 2 | |
| | Однонаправленные хеш-функции. Алгоритмы цифровой подписи | 2 | |
| | **Практическая работа** | **8** | |
| | Применение различных функций хеширования, анализ особенностей хешей | 2 | |
| | Применение криптографических атак на хеш-функции. | 2 | |
| | Изучение программно-аппаратных средств, реализующих основные функции ЭП | 2 | |
| | Изучение аутентификация данных. | 2 | |
| **Тема 3.5.** Алгоритмы обмена ключей и протоколы аутентификации | **Содержание** | **4** | ПК 1.2.<br>ПК 1.3<br>ПК 1.4<br>ОК 1– ОК 10 |
| | Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. | 2 | |
| | Взаимная аутентификация. Односторонняя аутентификация. | 2 | |
| | **Практическая работа** | **8** | |
| | Применение протокола Диффи-Хеллмана для обмена ключами шифрования. | 4 | |
| | Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos. | 4 | |
| **Тема 3.6.** Криптозащита информации в сетях передачи данных | **Содержание** | **6** | ПК 1.2.<br>ПК 1.3<br>ПК 1.4<br>ОК 1– ОК 10 |
| | Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. | 2 | |
| | Криптомаршрутизатор. Пакетный фильтр | 2 | |
| | Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP. | 2 | |
| **Тема 3.7.** Защита информации в электронных платежных системах | **Содержание** | **6** | ПК 1.2.<br>ПК 1.3<br>ПК 1.4<br>ОК 1– ОК 10 |
| | Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер | | |
| | Применение криптографических протоколов для обеспечения безопасности электронной коммерции. | | |
| | **Практическая работа** | **10** | |
| | Применение аутентификации по одноразовым паролям. | 2 | |

| | | | |
|---|---|---|---|
| | Реализация алгоритмов создания одноразовых паролей. | 2 | |
| | Применение криптографических протоколов для обеспечения безопасности электронной коммерции. | 2 | |
| | Изучение электронных платежных систем | 2 | |
| | Изучение программатора электронных пластиковых карт | 2 | |
| **Тема 3.8.** Компьютерная стеганография | **Содержание** | **6** | ПК 1.2. ПК 1.3 ПК 1.4 ОК 1– ОК 10 |
| | Скрытая передача информации в компьютерных системах. | 2 | |
| | Проблема аутентификации мультимедийной информации. Защита авторских прав. | 2 | |
| | Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ | 2 | |
| | **Практическая работа** | **8** | |
| | Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ | 4 | |
| | Реализация простейших стеганографических алгоритмов | 4 | |
| **Самостоятельная работа при изучении МДК.02.02** | | **18** | |
| 1. История развития криптографии | | | |
| 2. Программная реализация классических шифров | | | |
| 3. Оптимизация методов частотного анализа моноалфавитных шифров. | | | |
| 4. Программная реализация классических шифров | | | |
| 5. Методы механизации шифрования | | | |
| 6. Цифровое представление различных форм информации | | | |
| 7. Анализ современных симметричных криптоалгоритмов | | | |
| 8. Анализ современных асимметричных криптоалгоритмов | | | |
| 9. Программная реализация современных криптоалгоритмов | | | |
| 10. Сравнительный анализ функций хеширования | | | |
| 11. Аутентификация сообщений | | | |
| 12. Законодательство в области криптографической защиты информации | | | |
| 13. Перспективные направления криптографии | | | |
| **Промежуточная аттестация по МДК.02.02- дифференцированный зачет** | | **2** | |
| **Учебная практика** | | **108** | |
| **Виды работ:** | | | |
| 1. Установка операционной системы Windows на виртуальной машине. Использование редактора реестра. | | | |
| 2. Управление дисками из командной строки | | | |
| 3. Обеспечение безопасности папок и документов | | | |

| | | |
|---|---|---|
| 4. Реализация подсистем аутентификации в распространенных операционных системах. | | |
| 5. Аудит в Windows. | | |
| 6. Просмотр и работа с журналом аудита | | |
| 7. Противодействие взлому | | |
| 8. Работа со зловредными программами | | |
| 9. Архитектуры информационных сетей | | |
| 10. Изучение и обратное проектирование ПО. Способы изучения ПО: статическое и динамическое изучение | | |
| 11. Задачи защиты от изучения и способы их решения. Защита от отладки. | | |
| 12. Защита от дизассемблирования. Защита от трассировки по прерываниям. | | |
| 13. Изучение новых технологий хранения информации | | |
| 14. Статистика и анализ крупных утечек информации за год | | |
| 15. Поиск информации о новых видах атак на информационную систему | | |
| 16. Обзор современных программных и программно-аппаратных средств защиты | | |
| 17. Сравнительный анализ современных программных и программно-аппаратных средств защиты | | |
| 18. Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи | | |
| **Производственная практика** | **144** | |
| **Виды работ:** | | |
| 1. Анализ принципов построения систем информационной защиты производственных подразделений. | | |
| 2. Анализ принципов построения систем информационной защиты производственных подразделений. | | |
| 3. Анализ принципов построения систем информационной защиты производственных подразделений. | | |
| 4. Анализ принципов построения систем информационной защиты производственных подразделений. | | |
| 5. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. | | |
| 6. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. | | |
| 7. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. | | |
| 8. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. | | |
| 9. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; | | |
| 10. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; | | |
| 11. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; | | |

| | | |
|---|---|---|
| 12. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; | | |
| 13. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении | | |
| 14. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении | | |
| 15. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении | | |
| 16. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении | | |
| 17. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации | | |
| 18. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации | | |
| 19. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации | | |
| 20. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации | | |
| 21. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | | |
| 22. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | | |
| 23. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | | |
| 24. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. | | |
| **Экзамен по профессиональному модулю** | **12** | |
| **Всего:** | **724** | |

# 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- аудиовизуальный комплекс;
- комплект обучающего материала (комплект презентаций).

Оборудование лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- дистрибутив устанавливаемой операционной системы;
- виртуальная машина для работы с операционной системой (гипервизор);
- СУБД;
- CASE-средства для проектирования базы данных;
- инструментальная среда программирования;
- пакет прикладных программ.

Оборудование лаборатории и рабочих мест лаборатории сетей и систем передачи информации:

рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;

- стенды сетей передачи данных;
- структурированная кабельная система;
- эмулятор (эмуляторы) активного сетевого оборудования;
- программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно-аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

Реализация программы модуля предполагает обязательную учебную практику.

## 3.2. Информационное обеспечение обучения

**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:**

**Основные печатные источники**


1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2021.
2. Костров Б. В., Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2021.
3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 3-е изд.- М.: Горячая линия-Телеком, 2021.
4. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2021.
5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2022.
6. Синицын С.В., Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2022.
7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2022.
8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2022.


**Дополнительные печатные источники:**


1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2021.
2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2021. – 224 с.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 4-е изд. - СПб.: Питер, 2022 - 703 с.
4. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2022. - 88 с.
5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2022. – 1024 с.
6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2022. – 704 с.
7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2022

8. Кофлер М., Linux. Полное руководство – Питер, 2022. – 800 с.
9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2022
10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 4-е изд., испр.- М.: Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2022.- 531 с.
11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 6-е изд. – М.: Вильямс, 2022. – 656 с.
12. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2022.- 147 с.
13. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2022. – 544 с.
14. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2022. – 240 с.
15. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2022. – 672 с.
16. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2022. – 368 с.

**Периодические издания:**

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы 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. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
2. Информационный портал по безопасности www.SecurityLab.ru.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал www.biometrics.ru
5. Сайт журнала Информационная безопасность http://www.itsec.ru –

6. Сайт Научной электронной библиотеки www.elibrary.ru
7. Справочно-правовая система «Гарант» » www.garant.ru
8. Справочно-правовая система «Консультант Плюс» www.consultant.ru
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
10 .Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
11 .Федеральный портал «Российское образование www.edu.ru

# 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| **Код и наименование профессиональных и общих компетенций, формируемые 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 | тестирование,<br>экзамен квалификационный,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |
| 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 | тестирование,<br>экзамен квалификационный,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |
| 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 | тестирование,<br>экзамен квалификационный,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач, |

| | | |
|---|---|---|
| | | оценка процесса и результатов выполнения видов работ на практике |
| ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа. | Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа | тестирование,<br>экзамен квалификационный,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |
| 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 | тестирование,<br>экзамен квалификационный,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |
| 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. | Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак | тестирование,<br>экзамен квалификационный,<br>экспертное наблюдение выполнения лабораторных работ,<br>экспертное наблюдение выполнения практических работ,<br>оценка решения ситуационных задач,<br>оценка процесса и результатов выполнения видов работ на практике |

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только форсированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

| **Результаты (освоенные общие компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ОК 01. Выбирать способы решения задач профессионально й деятельности, применительно к различным контекстам. | - выбор метода и способа решения профессиональных задач с соблюдением техники безопасности и согласно заданной ситуации;<br>-оценка эффективности и качества выполнения согласно заданной ситуации | Наблюдение, мониторинг, оценка содержания портфолио студента.<br>Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях. |
| ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - эффективный поиск необходимой информации;<br>- информация, подобранная из разных источников в соответствии с заданной ситуацией | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.<br>Экспертная оценка содержания и правильности оформления реферативных и курсовых работ |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - решение стандартных и нестандартных профессиональных задач в области эксплуатации компонент подсистем безопасности автоматизированных систем; | Мониторинг и рейтинг выполнения работ на учебной и производственной практике.<br>Экспертная оценка работы студентов по самообразованию |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией;<br>- демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями. | Подготовка рефератов, докладов, сообщений, использование электронных источников.<br>Экспертная оценка и наблюдение при выполнении работ на теоретических занятиях, на учебной и производственной практике. |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом | - демонстрация позитивных коммуникативных навыков и социальной адаптации | Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях.<br>Наблюдение, мониторинг, оценка содержания портфолио |

| | | |
|---|---|---|
| особенностей социального и культурного контекста. | | студента. |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. | - демонстрация интереса к будущей профессии;<br>демонстрация целеустремленности, самообразования и саморазвития | Наблюдение за ролью обучающегося в группе; портфолио.<br>Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях.<br>Наблюдение, мониторинг, оценка содержания портфолио студента. |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - демонстрация качества принятых организационных решений<br>- готовность к частой смене технологий в профессиональной деятельности;<br>анализ инноваций в области профессиональной деятельности. | Деловые игры<br>-моделирование социальных и профессиональных ситуаций.<br>Семинары<br>Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций.<br>Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады. |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. | - оценка собственного продвижения, личностного развития. | Контроль графика выполнения индивидуальной самостоятельной работы обучающегося; открытые защиты творческих и проектных работ |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - использование основных видов современной вычислительной техники;<br>- эксплуатация и устранение типичных выявленных дефектов технических средств | Семинары<br>Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады.<br>Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций. |

| | | |
|---|---|---|
| | информатизации;<br>демонстрация результативной деятельности в области эксплуатации и технического сопровождения автоматизированных систем | |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках. | - использование пакетов прикладных программ для решения производственных задач<br>- использование базовых системных программных продуктов и пакетов прикладных программ;<br>-работа в интегрированной среде программирования | Семинары<br>Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций.<br>Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады. |
| ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. | - использование пакетов прикладных программ для решения производственных задач<br>- использование базовых системных программных продуктов и пакетов прикладных программ;<br>-работа в интегрированной среде программирования | Семинары<br>Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций.<br>Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады. |