

приложение 1.2
к ОПОП по специальности
10.02.05 Обеспечение информационной
безопасности автоматизированных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

2022г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупненной группы специальностей 10.00.00 Информационная безопасность.

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение Новосибирской области «Новосибирский профессионально-педагогический колледж».

Разработчики:

Елизова Ю.В., преподаватель

Рассмотрена и принята на заседании кафедры информационных технологий и дизайна

Протокол № 1 от 01.09.2022г.

Руководитель кафедры _____ О.Ю.Ануфриева

(подпись)

СОДЕРЖАНИЕ

| | |
|---|-----------|
| 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФФЕСИОНАЛЬНОГО МОДУЛЯ | 4 |
| 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ | 8 |
| 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ | 16 |
| 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ | 18 |

**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 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах 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 | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3 | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4 | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами |
| ОК 5 | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. |
| ОК 7 | Содействовать сохранению окружающей среды, ресурсосбережению, 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 | 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. |

1.1.2 Перечень профессиональных компетенций

| Код | Наименование видов деятельности и профессиональных компетенций |
|------------|--|
| ВД 2 | Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных систем |
| 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 Перечень личностных результатов:

| | |
|-------|---|
| ЛР 13 | Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности |
| ЛР 14 | Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности |
| ЛР 15 | Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем. |
| ЛР 16 | Выражающий активную гражданскую позицию, участвующий в формировании условий для успешного развития потенциала молодежи в интересах социально-экономического, общественно-политического и культурного развития региона |
| ЛР 17 | Способный генерировать новые идеи для решения профессиональных задач, перестраивать сложившиеся способы их решения, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов; позиционирующий как результативный и привлекательный участник трудовых отношений |
| ЛР 18 | Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению |
| ЛР 19 | Готовый к профессиональной конкуренции и конструктивной реакции на критику |
| ЛР 20 | Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством |
| ЛР 21 | Экономически активный, предприимчивый, готовый к самозанятости |

1.1.4 В результате освоения профессионального модуля обучающийся должен:

| | |
|-------------------------|--|
| Иметь практический опыт | <ul style="list-style-type: none"> - установка, настройка программных средств защиты информации в автоматизированной системе; - обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; - использование программных и программно-аппаратных средств для защиты информации в сети; - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; - решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; - применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; |
|-------------------------|--|

| | |
|-------|---|
| | <ul style="list-style-type: none"> - учет, обработка, хранение и передача информации, для которой установлен режим конфиденциальности; - работа с подсистемами регистрации событий; - выявление событий и инцидентов безопасности в автоматизированной системе. |
| Уметь | <ul style="list-style-type: none"> - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - использовать типовые программные криптографические средства, в том числе электронную подпись; - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - применять программные и программно-аппаратные средства для защиты информации в базах данных; - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - применять математический аппарат для выполнения криптографических преобразований; - применять средства гарантированного уничтожения 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 | <ul style="list-style-type: none"> - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа; - основные понятия криптографии и типовых криптографических методов и средств защиты информации. |

1.2 Количество часов на освоение программы профессионального модуля

Всего 527 часа

в том числе в формате практической подготовки 224 часа

Из них на освоение МДК.02 344 часа

в том числе самостоятельная работа 55 часа

практики, в том числе учебная 36 часов

производственная 108 часов

Промежуточная аттестация 39 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Тематический план профессионального модуля

| Коды профессиональных общих компетенций | Наименования разделов профессионального модуля | Объем профессионального модуля, ак. час. | | | | | | | | | | |
|---|--|--|----------------------------------|---|-------------|------------|----------|-----------|------------------|-----------|---------------------------|-------------------------------------|
| | | Суммарный объем нагрузки, час. | В т.ч. в форме практ. подготовки | Работа обучающихся во взаимодействии с преподавателем | | | | | | | | Самостоятельная работа ¹ |
| | | | | Обучение по МДК | | | | Практики | | | Консультации ² | |
| | | | | Всего | В том числе | | | Учебная | Производственная | | | |
| Промежут. аттест. | Лаборат. и практ. занятий | Курсовых работ (проектов) ³ | | | | | | | | | | |
| <i>1</i> | <i>2</i> | <i>3</i> | <i>4</i> | <i>5</i> | <i>6</i> | <i>7</i> | <i>8</i> | <i>9</i> | <i>10</i> | <i>11</i> | <i>12</i> | |
| ПК 2.1 ПК 2.2 ПК 2.3 ПК 2.5 ПК 2.6 ЛР 13-ЛР 21 ПК 2.4 | МДК.02.01 Раздел 1. Защита информации в автоматизированных системах программными и программно-аппаратными средствами | 272 | 166 | 236 | | 130 | 30 | 36 | | | 37 | |
| | МДК 02.02 Раздел 2. Криптографические средства защиты информации | 108 | 58 | 108 | | 58 | | | | | 18 | |
| | Производственная практика | 108 | | | | | | | 108 | | | |
| | Промежуточная аттестация | 39 | | | 39 | | | | | | | |
| | Всего: | 527 | 224 | 344 | 39 | 188 | 30 | 36 | 108 | | 55 | |

¹ Самостоятельная работа в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием междисциплинарного курса.

¹ Консультации вставляются в случае отсутствия в учебном плане недель на промежуточную аттестацию по модулю.

¹ Данная колонка указывается только для специальностей СПО.

2.2. Содержание обучения по профессиональному модулю (ПМ)

| Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК) | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) | | Объем в часах |
|---|--|--|---------------|
| 1 | 2 | | 3 |
| МДК.02.01 Защита информации в автоматизированных системах программными и программно-аппаратными средствами | | | |
| Раздел 1. Защита информации в автоматизированных системах программными и программно-аппаратными средствами | | | 206 |
| Тема 1.1 Назначение и возможности программно-аппаратных средств защиты информации | 1 | Инструктаж по ТБ. Обзор курса. Компьютерная система как объект защиты информации. | 18 |
| | 2. | Категории атак. | |
| | 3 | Способы выявления хакерских атак. | |
| | 4 | Службы информационной безопасности. Пассивная и активная защита. | |
| | 5 | Задачи обеспечения программно-аппаратной защиты. | |
| | 6 | Несанкционированный доступ к инф-и. Система управления доступом. | |
| | 7 | Средства защиты информации от НСД. | |
| | 8 | Методология разработки политики информационной безопасности предприятия. | |
| | 9 | Аудит информационной безопасности. Механизмы и службы защиты. | |
| | В том числе практических занятий | | |
| 1. | Полномочное и мандатное управление доступом. Управление доступа на основе ролей. | | |
| 2. | Разработка политики безопасности. | | |
| 3. | Регистрация событий (аудит). | | |
| Тема 1.2 Защищенная автоматизированная система | Содержание | | 4 |
| | 1. | Автоматизация процесса обработки информации. Функциональная модель системы защиты. | |
| 2. | Классификация технических каналов утечки информации, обрабатываемой ТСПИ и передаваемой по каналам связи. | | |
| В том числе практических занятий | | 12 | |
| 1. | Применение средств защиты информации от утечки по каналам ПЭМИН, по сети электропитания, ЛВС и ЭВМ. | | |
| 2. | Методы разграничения доступа. Типовые модели управления доступом. | | |
| 3. | Анализ различных программных решений для защиты сетевого периметра. | | |
| 4. | Средства диагностики сети. Основы построения защищенных сетей. | | |
| 5. | Системы обнаружения вторжений. | | |

| | | |
|--|--|-----------|
| | Самостоятельная работа | |
| | 1. Программно–аппаратные СЗИ по техническим каналам утечки. | 6 |
| | 2. Защита информации от утечки по сети электропитания и по каналам ПЭМИН. | |
| | 3. Идентификация и аутентификация. Строгая и биометрическая идентификация пользователей. | |
| Тема 1.3 Защита информации в операционных системах. | Содержание | |
| | В том числе практических занятий | |
| | 1. Защита паролей в Windows. | 34 |
| | 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. | |
| | 3. Настройка политики безопасности ОС Windows. | |
| | 4. Конфигурирование и настройка средств безопасности ОС. | |
| | 5. Администрирование ОС. Настройка межсетевых экранов Windows. | |
| | 6. Защита от взлома локальных учётных записей. Копирование и уничтожение информации. | |
| | 7. Работа в ОС Windows Server 2012. | |
| | 8. Создание домена в Active Directory. | |
| | 9. Файловая система OS Linux. Загрузка, первичные навыки работы. Форматирование системного вызова. | |
| | 10. Основные команды для работы в терминале Linux. | |
| | 11. Управление пользователями, сетью. Работа с процессами. | |
| | Самостоятельная работа | |
| 1. Общие сведения об ОС. Файловые системы Windows FAT32, NTFS, EFS. Файловые системы FXT2. | 14 | |
| 2. Типовые задачи администрирования. Способы взлома ОС Windows. | | |
| 3. Классификация способов защиты. Защита от отладки и дизассемблирования. | | |
| 4. Технологии межсетевых экранов. Классификация firewall-ов. | | |
| 5. Угрозы безопасности в ОС. IDS-системы. Основное назначение сервисов DNS. | | |
| 6. Защита информации в ОС Windows Server. Active Directory. | | |
| 7. Файловая система OS Linux. Основные концепции, принципы. | | |
| Тема 1.4 Программно-аппаратные средства защиты информации от утечек. | Содержание | |
| | В том числе практических занятий | |
| | 1. Настройки виртуальной среды Virtual Box. | 48 |
| | 2. Запуск гостевых виртуальных машин - ОС CentOS и Red Hat Linux. | |
| | 3. Установка СКЗ от внутренних угроз InfoWatch Traffic Monitor. | |
| | 4. Установка и настройка СУБД PostgreSQL. | |
| | 5. Установка компоненты СКЗ от ВУ InfoWatch Device Monitor. | |
| 6. Настройка ПО InfoWatch Traffic и Device Monitor. | | |

| | | | | |
|---|---|---|-----------|-----------|
| | 7. | Установка компоненты СКЗ от ВУ InfoWatch Crawler. | | |
| | 8. | Изучение настроек веб-консоли DLP-системы InfoWatch. | | |
| | 9. | Сканирование сетевого трафика. Передача информации ограниченного доступа. | | |
| | 10. | Мониторинг работы пользователей. Настройка регистрации событий в СКЗИ. | | |
| | 11. | Создание и проверка политик в консоли InfoWatch Device Monitor. | | |
| | 12. | Создание и разрешение инцидентов в IWТМ, используя Генератор трафика. | | |
| | 13. | Контроль и анализ информационных потоков. | | |
| | Самостоятельная работа | | | 10 |
| | 1. | DLP-системы. Схема развертывания DLP-системы. | | |
| | 2. | DLP-система InfoWatch. Состав, особенности. | | |
| | 3. | ПО «InfoWatch Traffic Monitor» и «InfoWatch Device Monitor». | | |
| | 4. | Установка и конфигурирование компонентов DLP-системы. Меры предосторожности. | | |
| | 5. | Вопросы виртуализации. Современные гипервизоры. | | |
| Тема 1.5 Программные и аппаратные средства защиты компьютерных информационных систем от несанкционированного доступа. | Содержание | | 8 | |
| | 1. | Реализация СЗИ. Структура СЗИ от несанкционированного копирования. | | |
| | 2. | Классификация систем защиты информации от несанкционированного доступа. | | |
| | 3. | Система защиты информации от НСД - SecretNet. Основные функции и возможности. | | |
| | 4. | Подходы к защите информационных систем. Аппаратные ключи. | 16 | |
| | В том числе практических занятий | | | |
| | 1. | Способы установки защитных механизмов в защищаемые программные модули. | | |
| | 2. | Применение СЗИ от НСД и несанкционированного копирования. | | |
| | 3. | Применение средств защиты информации от НСД «Secret Net». | | |
| | 4. | Запуск и регистрация в системе защиты. Реализация моделей разграничения доступа. | | |
| 5. | Применение СЗИ от НСД доступа «ПАК Соболев». | | | |
| 6. | Управление компонентами комплекса «Соболев». | | | |
| Тема 1.6 Мониторинг систем защиты | Содержание | | 9 | |
| | 1. | Сетевые анализаторы. Сканеры уязвимостей. | | |
| | 2. | Подключение к ОС по заданному сетевому протоколу. | | |
| | 3. | Компьютерные вирусы. Классификация и характеристики. | | |
| | 4. | Механизмы заражения компьютерными вирусами. Методы и средства защиты от компьютерных вирусов. | | |
| | 5. | Защита информации в базах данных. | | |
| | В том числе практических занятий | | 10 | |
| 1. | Структура антивирусной защиты предприятия. Функциональные требования. | | | |

| | | | |
|---|---|--|-----------|
| | 2. | Установка и предварительная настройка Антивируса Касперского. | |
| | 3. | Анализ мировых SIEM-систем. | |
| | 4. | Развертывание VPN. | |
| | Самостоятельная работа | | |
| | 1. | Виртуальная частная сеть VPN. | 2 |
| Тема 1.7 Нормативно-правовые акты в области информационной деятельности и деятельности по защите информации | Содержание | | |
| | В том числе практических занятий | | 4 |
| | 1. | Работа с государственным реестром сертифицированных СЗИ. | |
| | Самостоятельная работа | | |
| | 1. | Правовые и Конституционные основы обеспечения ИБ личности и государства. | 5 |
| | 2. | Виды нормативно-правовых актов в области защиты информации. | |
| | 3. | Гос.реестр сертифицированных средств защиты информации. | |
| Учебная практика по Разделу 1 Виды работ Применение программно-аппаратных средств обеспечения информационной безопасности АС. Диагностирование и обеспечение работоспособности программно-аппаратных средств обеспечения ИБ. Участие в обеспечении учёта, обработки, хранения и передачи конфиденциальной информации. Корпоративная защита от внутренних угроз на базе DLP–системы InfoWatch Traffic Monitor. Разработка политик безопасности в периметре организации на основе DLP–системы InfoWatch Traffic Monitor. Мониторинг и регистрация сведений, необходимых для защиты объектов информатизации, с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. Аутентификация/ идентификация пользователей. Администрирование системы корпоративной защиты информации. | | | 36 |
| Курсовой проект (работа) по МДК 02.01 Тематика курсового проекта 1. Оценка защищённости ОС Windows XP Professional (Windows 10) в соответствии со стандартами ISO. 2. Анализ методов изучения поведения нарушителей безопасности компьютерных систем. 3. Программно-аппаратные средства защиты информационных ресурсов от несанкционированного использования и копирования. 4. Варианты решения антивирусной защиты корпоративной сети. 5. Аутентификация пользователей на основе их способностей к запоминанию отображаемой на короткое время информации. 6. Корпоративная защита от внутренних угроз на базе DLP–системы. 7. Разработка политики безопасности предприятия. | | | 30 |

| МДК.02.02 Криптографические средства защиты информации | | |
|--|--|------------|
| Раздел 2. Криптографические средства защиты информации | | 108 |
| Тема 2.1 Основные понятия криптографической защиты информации | Содержание | 8 |
| | 1. Инструктаж по технике безопасности. Криптография, криптоанализ, стенография, кодирование. | |
| | 2. Основные понятия криптографической защиты информации. | |
| | 3. Оценка надёжности криптоалгоритмов. | |
| | 4. Классификация криптографических методов защиты информации. | 16 |
| | В том числе практических занятий | |
| | 1. Шифрование методом Вижинера. | |
| | 2. Шифрование методом перестановки. | |
| | 3. Шифрование методом Вернама. | |
| | 4. Шифрование методом гаммирования. | |
| | 5. Алгоритм Евклида для нахождения НОД чисел. | |
| | 6. Проверка чисел на простоту. | |
| | 7. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. | |
| 8. Алгоритм быстрого возведения в степень по модулю. | | |
| Самостоятельная работа | 4 | |
| 1. Методы перестановки (транспозиции). | | |
| | 2. Шифрование методом гаммирования. Метод Вернама. | |
| Тема 2.2 Симметричные криптосистемы шифрования | Содержание | 4 |
| | 1. Понятия симметричной криптосистемы. | |
| | 2. Поточные и блочные шифры. | 10 |
| | В том числе практических занятий | |
| | 1. Практические реализации итерационных блочных шифров. | |
| | 2. Российский стандарт шифрования ГОСТ 28147-89. | |
| | 3. Схема шифрования в алгоритме ГОСТ 28147-89. | |
| | 4. Стандарт симметричного шифрования AES RIJNDAEL. | |
| | Самостоятельная работа | 4 |
| | 1. Алгоритм шифрования DES. | |
| | 2. Основные режимы работы блочного симметричного алгоритма | |
| Тема 2.3 Асимметричные криптосистемы | Содержание | 8 |
| | 1. Понятия асимметричной криптосистемы. | |

| | | | | |
|---|---|---|----|----|
| шифрования | 2. | Алгоритм шифрования RSA. | 14 | |
| | 3. | Функция хеширования. | | |
| | 4. | Генераторы псевдослучайных чисел. | | |
| | В том числе практических занятий | | | |
| | 1. | Шифрование с помощью алгоритмов Диффи-Хеллмана и Эль Гамала. | | |
| | 2. | Шифрование методом RSA. | | |
| | 3. | Получение хэш-кода сообщения. | | |
| | 4. | Схема хеширования по алгоритму ГОСТ Р 34.11-94. | | |
| | 5. | Генерация псевдослучайных чисел различными методами. | | |
| | Самостоятельная работа | | | |
| 1. | Отечественный стандарт хеширования ГОСТ Р 34.11-94. | 4 | | |
| 2. | Алгоритмы Диффи-Хеллмана и Эль Гамала. | | | |
| Тема 2.4 Электронная цифровая подпись | Содержание | | 8 | |
| | 1. | Электронная цифровая подпись. | | |
| | 2. | Стандарты на алгоритмы цифровой подписи. | | |
| | 3. | Российский стандарт цифровой подписи ГОСТ Р 34.10-94. | | |
| | 4. | Новый Российский стандарт цифровой подписи ГОСТ Р 34.10.2001. | | |
| | В том числе практических занятий | | | |
| | 1. | Формирование электронной подписи на основе алгоритмов Эль Гамала и RSA. | | 12 |
| | 2. | Формирование электронной подписи на основе алгоритмов ГОСТ Р 34.10-94 и 34.10-2001. | | |
| | 3. | Использование программы PGP для формирования и проверки электронной подписи. | | |
| | Самостоятельная работа | | | 2 |
| 1. | Усиленная квалифицированная электронная подпись | | | |
| Тема 2.5 Новые возможности криптографии | Содержание | | 4 | |
| | 1. | Совершенно секретные криптосистемы. | | |
| | 2. | Шифрование, помехоустойчивое кодирование и сжатие информации. | 6 | |
| | В том числе практических занятий | | | |
| | 1. | Совершенные криптосистемы. | | |
| | 2. | Анализ безопасности протоколов обмена информацией. | 4 | |
| | 3. | Перспективы развития криптографических методов защиты. Причины ненадёжности криптосистем. Квантовая криптография. | | |
| | Самостоятельная работа | | 4 | |
| | 1. | Проблема аутентификации. Инфраструктура открытых ключей. | | |
| | 2. | Электронная цифровая подпись на основе алгоритмов Эль Гамала и RSA. | | |

| | |
|---|------------|
| <p>Производственная практика по Разделу 2</p> <p>Виды работ</p> <p>Рассмотреть на практике основные положения политики информационной безопасности предприятия.</p> <p>Администрирование подсистем безопасности автоматизированных информационных систем.</p> <p>Анализ и участие в обеспечении учёта, обработки, хранения и передачи конфиденциальной информации.</p> <p>Применение программно-аппаратных средств обеспечения информационной безопасности.</p> <p>Настройка межсетевых экранов.</p> <p>Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование.</p> <p>Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств.</p> <p>Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации.</p> <p>Корпоративная защита от внутренних угроз.</p> <p>DLP-системы. Схема развертывания и установки DLP системы.</p> <p>Сканирование сетевого трафика. Контроль передачи информации ограниченного доступа.</p> <p>SIEM-системы. Средства анализа и управления данными.</p> <p>Использование и оформление технической документации в соответствии с действующими нормативными актами.</p> <p>Применение нормативно-правовых актов, нормативно-методических документов по обеспечению информационной безопасности программно-аппаратными средствами.</p> | 108 |
| <p>Промежуточная аттестация</p> | 39 |
| <p>Всего</p> | 527 |

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

лаборатория программно-аппаратных средств обеспечения информационной безопасности.

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

- компьютеры – рабочее место студента;
- мультимедийный компьютер – рабочее место преподавателя;
- мультимедиа проектор, проекционный экран;
- доска;
- принтер лазерный;
- сканер;
- локальная сеть колледжа, электронная почта, выход в Интернет;
- программное обеспечение общего и профессионального назначения;
- комплект учебно-методической документации.

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендованные ФУМО, для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список, может быть дополнен новыми изданиями.

3.2.1 Основные печатные издания

1. Гагарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. – 384 с. - (Профессиональное образование)

2. Информационная безопасность: учебник / Мельников В.П., под ред., Куприянов А.И., Васильева Т.Ю. — Москва: КноРус, 2020. — 371 с. — (для бакалавров). — ISBN 978-5-406-07695-8. — URL: <https://book.ru/book/932908> — Текст: электронный.

3. Партыка Т.Л., Попов И.И. Информационная безопасность: учебное пособие для студентов учреждений среднего профессионального образования. – 5-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА – М, 2016. – 432 с.: ил. – (Профессиональное образование).

4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с. - (Профессиональное образование).

3.2.2 Дополнительные источники

1. Гришин, В. Н. Информационные технологии в профессиональной деятельности [Текст]: учебник/ Е. Е. Панфилова. - М.: ФОРУМ: ИНФРА-М, 2005. - 416 с.: ил. - (Профессиональное образование).

2. Информационные технологии [Текст]: учебник/ О.Л. Голицына, Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - М.: ФОРУМ: ИНФРА-М, 2006. - 544 с.: ил. - (Профессиональное образование).

3. Максимов, Н. В. Компьютерные сети [Текст]: учебное пособие/ Н. В. Максимов, И. И. Попов. - М.: ФОРУМ: ИНФРА-М, 2004. - 336 с.: ил. - (Профессиональное образование).

4. Михеева, Е. В. Информационные технологии в профессиональной деятельности [Текст]: учебное пособие/ Е. В. Михеева. - 2 изд., стереот. - М.: Академия, 2005. - 384 с.: ил. - (Среднее профессиональное образование).

5. Румянцева, Е. Л. Информационные технологии [Текст]: учебное пособие/ Е. Л. Румянцева, В. В. Слюсарь; ред. Л. Г. Гагарина. - М.: ФОРУМ: ИНФРА-М, 2007. - 256 с.: ил. - (Профессиональное образование).

6. Мельников, В. П. Информационная безопасность [Текст]: учебное пособие/ В.П. Мельников, С.А. Клейманов, А.М. Петраков; под ред. С.А. Клейманов. - М.: Академия, 2005. - 333 с.: ил. - (Среднее профессиональное образование).

Периодические издания

1. Информационная безопасность [Текст]: научный журнал. - М.: [б. и.], 2016. - Выходит ежеквартально.

2. Информатика - первое сентября [Текст]: учебно-методический журнал для учителей информатики. - М.: Первое сентября, 2016. - Выходит ежемесячно.

3. Мой друг компьютер [Текст]: простыми словами о том, что вам кажется сложным; газета. – Нижний Новгород: ООО "Издательство "Газетный мир", 2016. – Выходит ежемесячно.

Электронные источники

1. Поисковые системы Интернет: Яндекс, Google, Rambler

2. <http://fstec.ru> - Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00

Формы проведения учебных занятий и практики - лабораторная, компьютерный класс, предусмотрена дистанционная форма (работа через Интернет-ресурсы).

В условиях дистанционного обучения:

- инструктаж и выдача задания производится в форме телеконференции в программе Zoom;

- вся необходимая документация высылается по электронной почте;

- обратная связь и консультации осуществляются в приложении Вотсап, Skype, Вконтакте и по электронной почте;

- выполненные задания собираются в архив и отправляются на облако;

- отчёты по практике распечатываются;

- защита учебной практики, зачета, экзамена осуществляется в форме телеконференции в программе Skype или Zoom.

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. | - обеспечение безопасности в автоматизированных системах | Текущий контроль в форме: - защиты лабораторных и практических занятий; |
| ПК 2.2 Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами | - соблюдение сроков выполнения задания - работоспособность программного обеспечения | Зачеты по учебной практике и по каждому из разделов профессионального модуля |
| ПК 2.3 Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. | - соответствие отчета проверки эффективности стандартам и нормативной документации по обеспечению информационной безопасности программно-аппаратными средствами - соблюдение сроков выполнения задания - работоспособность программного обеспечения | Квалификационный экзамен по модулю Защита курсовой работы |
| ПК 2.4 Осуществлять обработку, хранение и передачу информации ограниченного доступа. | - соблюдение сроков выполнения задания - работоспособность программного обеспечения | |
| ПК 2.5 Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств | - работоспособность программно-аппаратного обеспечения | |
| 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 | - соответствие нормативным правовым актам по обеспечению информационной безопасности программно-аппаратными средствами | |

| | | |
|--|--|---|
| ОК.01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | - демонстрация интереса к будущей профессии | Интерпретация результатов наблюдений за деятельностью студентов в процессе освоения образовательной программы |
| ОК.02 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - выбор и применение методов и способов решения профессиональных задач в области обеспечения информационной безопасности программно-аппаратными средствами - оценка эффективности и качества выполнения | |
| ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие. | - решение стандартных и нестандартных профессиональных задач в области обеспечения информационной безопасности программно-аппаратными средствами | |
| ОК.04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами | - эффективный поиск необходимой информации; - использование различных источников, включая электронные источники и интернет | |
| ОК.05 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | - применение информационных технологий для осуществления информационной безопасности | |
| ОК.06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. | - взаимодействие со студентами, преподавателями и мастерами в ходе обучения - работа в малых группах | |
| ОК.07 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - самоанализ и коррекция результатов собственной работы; - анализ результатов выполнения практических заданий, лабораторных работ | |
| ОК.08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | - организация самостоятельных занятий при изучении профессионального модуля | |

| | | |
|---|--|---|
| ОК.09 Использовать информационные технологии в профессиональной деятельности. | - анализ инноваций в области информационной безопасности; - умение внедрять новые программные продукты | |
| ОК.10 Пользоваться профессиональной документацией на государственном и иностранном языках. | - применение средств математической логики для решения логических задач | |
| ОК.11 Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. | - разработка программного обеспечения | |
| ЛР 13-21 | Выполнение работ в соответствии с установленными регламентами с соблюдением правил безопасности труда, санитарными нормами | экспертное наблюдение выполнения практических работ |