

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ»

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»



УТВЕРЖДАЮ

Заместитель директора по УМР

 Е.Ю. Кузнецов

«28» апреля 2023 г.

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ**

по специальности 11.02.15 Инфокоммуникационные сети и системы связи

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 7

«27» апреля 2023 г.

Председатель ПЦК  /Е.Ю. Кузнецов/

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного Приказом Минпросвещения России от 05.08.2022 № 675.

Разработчик:

Савинов Александр Николаевич, канд. техн. наук, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «ПГТУ».

Рецензент (внутренний)

Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа «Политехник».

Рецензент (внешний)

Еросланов С.Г., директор сервисного центра г. Йошкар-Ола филиала Республики Марий Эл ПАО «Ростелеком».

СОДЕРЖАНИЕ

1. АННОТАЦИЯ
2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. АННОТАЦИЯ

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи является базовой профессиональной подготовки ППССЗ СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи.

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

иметь практический опыт в:

- анализировании сетевой инфраструктуры;
- выявлении угрозы и уязвимости в сетевой инфраструктуре,
- разрабатывании комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи,
- осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи;
- использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.

уметь:

- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
- проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;
- определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;
- осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
- выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты;
- выполнять тестирование систем с целью определения уровня защищенности;
- определять оптимальные способы обеспечения информационной безопасности;
- проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;
- проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;
- разрабатывать политику безопасности сетевых элементов и логических сетей;
- выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
- производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;
- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

- защищать базы данных при помощи специализированных программных продуктов;
- защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами;

знать:

- принципы построения информационно-коммуникационных сетей;
- международные стандарты информационной безопасности для проводных и беспроводных сетей;
- нормативно - правовые и законодательные акты в области информационной безопасности;
- акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
- технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
- способы и методы обнаружения средств съёма информации в радиоканале;
- классификацию угроз сетевой безопасности;
- характерные особенности сетевых атак;
- возможные способы несанкционированного доступа к системам связи,
- правила проведения возможных проверок согласно нормативным документам ФСТЭК;
- этапы определения конфиденциальности документов объекта защиты;
- назначение, классификацию и принципы работы специализированного оборудования;
- методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;
- методы и средства защиты информации в телекоммуникациях от вредоносных программ;
- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов;
- методы и способы защиты информации, передаваемой по кабельным направляющим системам;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- средства защиты различных операционных систем и среды передачи информации;
- способы и методы шифрования (кодирование и декодирование) информации.

Общий объем учебной нагрузки по профессиональному модулю составляет 302 часа, нагрузка во взаимодействии с преподавателем составляет 99 часов, самостоятельной работы – 21 час, учебной практики – 2 нед. /72 часа, производственной практики – 2 нед. /72 часа.

Содержание профессионального модуля включает изучение следующих тем:

МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи.

Тема 1. Основы безопасности информационных технологий.

Тема 2. Обеспечение безопасности информационных технологий.

Тема 3. Обеспечение безопасности стандартными средствами защиты.

Тема 4. Криптографическая защита информации.

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

| Код | Наименование результата обучения |
|--------|---|
| ПК 3.1 | Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. |
| ПК 3.2 | Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. |
| ПК 3.3 | Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. |
| ОК 01 | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам. |
| ОК 02 | Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности. |
| ОК 03 | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях. |
| ОК 04 | Эффективно взаимодействовать и работать в коллективе и команде. |
| ОК 05 | Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста. |
| ОК 06 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. |
| ОК 07 | Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях. |
| ОК 08 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. |
| ОК 09 | Пользоваться профессиональной документацией на государственном и иностранном языках. |

Текущий контроль проводится в форме оценки тестирования, решения ситуационных задач и выполнения лабораторных работ.

Форма промежуточной аттестации – дифференцированный зачет, экзамен, экзамен (квалификационный).

2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Место профессионального модуля в структуре программы подготовки специалистов среднего звена:

Профессиональный модуль ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи входит в общепрофессиональный цикл, профессиональной подготовки ППССЗ и реализуется в 6 и 7 семестре.

2.2. Цель и планируемые результаты освоения профессионального модуля

| Код ПК, ОК | Умения | Знания |
|---|--|---|
| ПК 3.1 ПК 3.2 ПК 3.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 06 ОК 07 ОК 08 ОК 09 | <ul style="list-style-type: none">– классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;– проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;– определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;– осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;– выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты;– выполнять тестирование систем с целью определения уровня защищенности;– определять оптимальные способы обеспечения информационной безопасности;– проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;– проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;– разрабатывать политику безопасности сетевых элементов и логических сетей;– выполнять расчет и установку специализированного оборудования для обеспечения максимальной | <ul style="list-style-type: none">– принципы построения информационно-коммуникационных сетей;– международные стандарты информационной безопасности для проводных и беспроводных сетей;– нормативно - правовые и законодательные акты в области информационной безопасности;– акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;– технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;– способы и методы обнаружения средств съема информации в радиоканале;– классификацию угроз сетевой безопасности;– характерные особенности сетевых атак;– возможные способы несанкционированного доступа к системам связи,– правила проведения возможных проверок согласно нормативным документам ФСТЭК;– этапы определения конфиденциальности документов объекта защиты;– назначение, классификацию и принципы работы специализированного оборудования;– методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;– методы и средства защиты информации в телекоммуникациях от вредоносных |

| | | |
|--|--|--|
| | <p>защищенности сетевых элементов и логических сетей;</p> <ul style="list-style-type: none"> – производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; – конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; – защищать базы данных при помощи специализированных программных продуктов; – защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами. | <p>программ;</p> <ul style="list-style-type: none"> – технологии применения программных продуктов; – возможные способы, места установки и настройки программных продуктов; – методы и способы защиты информации, передаваемой по кабельным направляющим системам; – конфигурации защищаемых сетей; – алгоритмы работы тестовых программ; – средства защиты различных операционных систем и среды передачи информации; – способы и методы шифрования (кодирование и декодирование) информации. |
|--|--|--|

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

3.1. Тематический план профессионального модуля

| Код профессиональных компетенций | Наименования разделов профессионального модуля | Всего часов | Объем времени, отведенный на освоение междисциплинарного курса (курсов) | | | | | Практика | |
|----------------------------------|---|-------------|---|--|---|-------------------------------------|---|----------------|--|
| | | | Обязательная аудиторная учебная нагрузка обучающегося | | | Самостоятельная работа обучающегося | | Учебная, часов | Производственная (по профилю специальности),** часов |
| | | | Всего, часов | в т.ч. лабораторные работы и практические занятия, часов | в т.ч., курсовая работа (проект), часов | Всего, часов | в т.ч., курсовая работа (проект), часов | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| ПК 3.1 ПК 3.2 ПК 3.3 | МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи. | 302 | 99 | 60 | | 21 | | | |
| ПК 3.1 ПК 3.2 ПК 3.3 | Учебная практика, часов | 72 | | | | | | 72 | |
| ПК 3.1 ПК 3.2 ПК 3.3 | Производственная практика, часов | 72 | | | | | | | 72 |
| Всего: | | 446 | 99 | 60 | | 21 | | 72 | 72 |

3.2. Тематический план и содержание профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

| 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 | Формирующие компетенции |
|---|---|--|-------------|---|
| 1 | 2 | | 3 | 4 |
| ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи. | | | 302 | ПК 3.1 ПК 3.2 ПК 3.3 ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 06 ОК 07 ОК 08 ОК 09 |
| МДК. 03.01 Защита информации в инфокоммуникационных системах и сетях связи. | | | 140 | |
| Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи. | | | | |
| Тема 1.1. Основы безопасности информационных технологий. | Содержание учебного материала | | 2 | |
| | 1 | Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий. | | |
| | 2 | Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. | 4 | |
| | 3 | Угрозы безопасности информационных технологий. Классификация угроз безопасности. | 2 | |
| | 4 | Принципы обеспечения безопасности информационных технологий Принципы построения системы обеспечения безопасности информации в автоматизированной системе. | 4 | |
| | Лабораторные занятия | | 2 | |
| | 1 | Анализ современных угроз ИБ. | | |
| | 2 | Проектирование границ защиты. | | |
| | 3 | Применение сертификатов для аутентификации и авторизации. | 4 | |
| | Тема 1.2. Обеспечение безопасности информационных технологий. | Содержание учебного материала | | |
| 1 | | Особенности обеспечения информационной безопасности в компьютерных сетях. Спецификация средств защиты в компьютерных сетях. | | |
| 2 | | Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование. | 4 | |

| 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 | Формирующие компетенции |
|---|---|---|-------------|-------------------------|
| 1 | 2 | | 3 | 4 |
| | 3 | Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей. | 4 | |
| | Лабораторные занятия | | 6 | |
| | 1 | Установка СЗИ (На примере IWTM). | | |
| | 2 | Установка межсетевого экрана. | 6 | |
| | 3 | Настройка правил фильтрации трафика DLP системой. | 6 | |
| | 4 | Настройка уровней доступа к различным подсетям (Применяется firewall). | 6 | |
| Тема 1.3. Обеспечение безопасности стандартными средствами защиты. | Содержание учебного материала | | 4 | |
| | 1 | Локальные политики безопасности. | | |
| | Лабораторные занятия | | 4 | |
| | 1 | Настройка локальных политик (windows системы). | | |
| | 2 | Создание пользователей, административная, пользовательская, гостевая учетные записи (windows системы). | 4 | |
| | 3 | Создание пользователей, права суперпользователя, ограничения пользователей, права доступа (unix системы). | 8 | |
| Тема 1.4. Криптографическая защита информации. | Содержание учебного материала | | 2 | |
| | 1 | Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных. | | |
| | 2 | Симметричные криптосистемы. Ассиметричные криптосистемы. | 2 | |
| | 3 | Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом. | 2 | |
| | 4 | Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа. | 5 | |
| | Лабораторные занятия | | 4 | |
| | 1 | Шифрование данных симметричными и асимметричными алгоритмами. | | |

| 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 | Формирующие компетенции |
|---|---|--|-------------|-------------------------|
| 1 | 2 | | 3 | 4 |
| | 2 | Криптоанализ. | 4 | |
| | 3 | Шифрование трафика, шифрование данных. | 4 | |
| | Самостоятельная работа обучающихся по Разделу 1. | | 21 | |
| | 1 | <p>1. Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре.</p> <p>2. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа.</p> <p>3. Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.</p> <p>4. Применение различных программ для оперативного и гарантированного восстановления информации на ПК.</p> <p>5. Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации.</p> <p>6. Разработка комплекса организационно-административной защиты от вредоносных программ.</p> <p>7. Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте.</p> <p>8. Применение подсистемы безопасности WINDOWS XP/Vista/7 для предотвращения несанкционированного доступа к защищаемой информации.</p> | | |

| 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 | Формирующие компетенции |
|---|---|-------------|-------------------------|
| 1 | 2 | 3 | 4 |
| Учебная практика Виды работ: <ul style="list-style-type: none"> - установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов; - установка и настройка типовых программно-аппаратных средств защиты информации; - использование программно-аппаратных и инженерно-технических средств; - настройка, регулировка и ремонт оборудования средств защиты; - выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой; - проведение типовых операции настройки средств защиты операционных систем; - проведение аттестации объектов защиты; - определение источников несанкционированного доступа, исходя из модели угроз; - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта; - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств; - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК; - защита информации организационными методами в соответствии с инструкциями на объекте. | | 72 | |
| Производственная практика Виды работ: <ul style="list-style-type: none"> - участие в создании комплексной системы защиты на предприятии; - применение программно-аппаратных средств защиты информации на предприятии; - применение инженерно-технических средств защиты информации на предприятии; - применение криптографических средств защиты информации на предприятии. | | 72 | |
| Всего | | 302 | |
| Консультации | | 2 | |
| Промежуточная аттестация | | 36 | |
| Курсовая работа | | - | |
| Учебная практика | | 72 | |
| Производственная практика (по профилю специальности) | | 72 | |

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Кабинет компьютерного моделирования

Комплект мебели для учебного процесса.

Мультимедийное оборудование: компьютеры – 12 шт.: ПК 3 - ICL RAY S902.3, монитор ViewSonic VA2038W-LED; монитор 19" ViewSonic TFT 19" VA916; систем. блок P-Athlon64 X2 6000/1024*2М6/320 Gb/клавиатура+мышь+коврик; сканер MUSTEK Bear Paw 2400; прин-тер Canon LBP-1120; проектор мультимедийный Hitachi; калькуляторы.

Программное обеспечение: 1С: Документооборот 8 КОРП (лицензия №75027601); 1С:Предприятие 8. Комплект для обучения (лицензия №8922961); Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2023_СВ_3 от 29.12.2022г); КОМПАС-3D V19 (лицензия №Вг-20-00154); LABVIEW (лицензия №M75X89867); Мой Офис Образование (договор № 2350/2017).

Средства обучения: учебная доска, справочные пособия и дидактический материал, медиатека (мультимедиа разработки и презентации к урокам), экран.

Лаборатория информационной безопасности телекоммуникационных систем

Комплект мебели для учебного процесса.

Мультимедийное оборудование: персональные компьютеры – 22 шт., проектор мультимедийный Hitachi CP-X1250, разветвитель видеосигнала; принтер HP LaserJet Professional P1102.

Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); анти-вирусный программный комплекс: Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); ком-плект ГАРАНТ–Мастер (лицензия №12–40272–000898); программные и программно-аппаратные средства обнаружения вторжений (Snort 2.9 (свободно распр. ПО), Nmap 7.8 (свободно распр. ПО); средства уничтожения остаточной информации в запоминающих устройствах («СГУ–2» демоверсия (свободно распр. ПО); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); Справочная правовая система «Консультант Плюс» (контракт №2023_СВ_3 от 29.12.2022г); программные средства выявления уязвимостей в АС и СБТ (Tenable Nessus® vulnerability scanner (свободно распр. ПО), Metasploit Framework (сво-бодно распр. ПО); программные средства криптографической защиты информации (Крипто-Про CSP 5.0 (лицензионный

контракт №010/IO20-002792 от 28.08.20), ViPNet CSP 4 (свободно-распространяемое); программные средства защиты среды виртуализации (VM Monitor (свободно распр. ПО), Zabbix (свободно распр. ПО).

Средства обучения: комплект наглядных пособий «Технические средства информатизации», техническая документация на технические средства информатизации, комплект презентаций; анализатор линейных коммуникаций ULAN-2; приёмник «Скорпион» поисковый, скоростной Ver 3.5; контрольное устройство ТЕСТ-031; многофункциональный поисковый прибор ST 031; нелинейный локатор SEL SP-61/М «Катран»; указатель проводки UP-7; генератор шума ГШ-2500; комплекс защиты информации в составе PCI-плата, ПО SN-5, считыватель, 2 идентификатора; комплекс защиты информации Secret Net 5.0; программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности (комплекс защиты информации Secret Net 5.0, комплекс защиты информации Secret Disc 4.0 аппаратный комплекс АККОРД - AMD3 - 5.5, аппаратный комплекс АККОРД -AMD3 - 5MX, аппаратный комплекс АККОРД -AMD3 — 5.5 Е, аппаратный комплекс СЗИ НСД АККОРД –AMD, подсистема распределённого аудита и управления «Аккорд-РАУ» (2 CD + ТМ ключ DS-1996), аппаратно-программный модуль доверенной загрузки с удалённым управлением для шины PCI-Express M-526E1 (АПМДЗ-УМ1 исполнение 1, КРИПТОН-ЗАМОК/Е) – 3 шт.); система вибро-акустической защиты «Соната-АВ»; устройство защиты «Соната-PC2»; устройство защиты «Соната-Р2»; виброизлучатель ВИ-45 – 5шт.; адаптер DWA-160-10 шт; DAP-2310 – 5шт.; DES-3200-28 – 8шт.; DES-3810-28 -2шт.; коммутатор D-Link DES-1005 – 5шт.; коммутатор D-Link DIR-615 – 5 шт.; коммутатор D-Link DES-1100-16 -5 шт.; кримпер NT-2008AR; кабельный тестер NCT-1; тестер кабельный TC-NT2; SMART-Cart Алладин – 2шт; ASEDrive IIIe V2C- 2 шт.; электронный ключ eToken – 8шт.; программные средства криптографической защиты информации (ПСКЗИ «Шипка 2.0» (диск + УСБ-устройство) -5шт); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (3 CD); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (2 CD)- 3 шт; программно-аппаратный комплекс «Соболь» (PCI-плата,CD-диск ПО, соединитель) – 3 шт.; экран настенный 200*200см Braun Roll Vision.

Лаборатория телекоммуникационных систем

Комплект мебели для учебного процесса.

Мультимедийное оборудование: системный блок CEL D-341 FAN/ASUS S-775/512 M/160.0G/DVD+-RW; антенна M102 в компл. с кабелем ВЧ TNCm-SMAm; антенный коммута-тор RK-318+RU-005A; внешний накопитель флешка USB TRANSCEND Jetflash 780 64 Gb; Монитор 19"Samsung 940N (LKSB) TFT, 2 шт.; МФУ 3210V_N Xerox Work Centre 3210; МФУ Canon Laser Base MF 3228 (копир.принтер.сканер) A4; ноутбук Dell Latitude E6520 Intel Core I5 Processor 2520M 15,6", 2 шт.; ноутбук Samsung NP -RF 511-S02RU 15,6"; ПК S404,2 400W/Intel Core i3 540/клава.,мышь,монит. 21,5" VA2248-LED; ПК H404,2 420W/Intel Core i3 540/клава.,мышь,монит. 21,5" VA2248-LED, 2 шт.; приемник IC-R75; систем.блок АМД3000+(512*2)/160Gb/DVD+RWrkfd/+мышь+коврик+клава.

Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); Комплект ПО для решения основных пользовательских задач (свободно распространяемое ПО); справочная правовая система «Консультант Плюс» (контракт №2023_СВ_3 от 29.12.2022г).

Средства обучения: кварцевый генератор "Астра" 10 МГц; комплекс лабораторного оборудования "Программируемая платформа для ВЧ-приложений" для работы в диапазоне частот 1-250МГц; лабораторный комплект по цифровой обработке сигналов; система сбора и анализа данных и управления; стандарт частоты GPS-12 RG в комплекте с антенной ACM-03 и кабелем; телевизор LED 42" LG 42LS; точка доступа Cisco AIR-CAP 1602I-R-K9; универсальная приёмо-передающая платформа для проектирования СВЧ-систем компл.mgxc2; устройство частотно времен-ной синхронизации по сигналам СНС ГЛОНАС и GPS NAVSTAR СН-3833; учебно-научно исслед.комплекс УНИК (Сверхширокополосн. беспроводн.сенсорные сети); учебно-научно исслед.комплекс УНИК (Сверхширокополосн. беспроводн.сенсорные сети) ; экран на штативе 180x180 см., управляемый коммутатор L2-2 шт., управляемый межсетевой экран-маршрутизатор L3-2 шт., комплект SFP-модулей FTTx для коммутаторов и маршрутизаторов, конвертеры 2 шт., мультиплексоры 2 шт., комплекты пассивных элементов для подключения абонентских терминалов и выполнения кроссировки, набор инструментов для выполнения кроссировочных работ.

Договоры о практической подготовке:

АО «Марийский машиностроительный завод» Договор № 1/2021 от 01.02.2021 – бессрочный.

Филиал ПАО «Ростелеком» в Республике Марий Эл Договор № 83/2021 от 27.01.2021 - бессрочный.

4.2. Учебно-методическое и информационное обеспечение обучения

Основная и дополнительная литература

| № п/п | Список используемой литературы (печатные издания, электронные издания за последние 5 лет) | Количество экземпляров, имеющих в библиотеке, или ссылка на ЭБС |
|---------------------------|---|---|
| ОСНОВНАЯ ЛИТЕРАТУРА | | |
| 1. | Гилязова, Р.Н. Информационная безопасность. Лабораторный практикум: учебное пособие для СПО / Р. Н. Гилязова. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 44 с. — ISBN 978-5-8114-8249-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/173796 (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей. | электронный ресурс |
| 2. | Никифоров, С.Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие / С. Н. Никифоров. — Санкт-Петербург: Лань, 2020. — 96 с. — ISBN 978-5-8114-5720-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/146802 (дата обращения: 27.11.2020). — Режим доступа: для авториз. пользователей. | электронный ресурс |
| 3. | Партыка, Т.Л. Вычислительная техника: учебное пособие / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - Москва: ФОРУМ: ИНФРА-М, 2022. - 445 с.: ил. - (Среднее профессиональное образование). - ISBN 978-5-00091-510-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1703191 (дата обращения: 10.09.2023). | электронный ресурс |
| 4. | Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации: учебник / сост. И.Г. Дровникова, А.В. Калач, И.И. Лившиц [и др]. - Воронеж: Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 29.08.2023). — Режим доступа: по подписке. https://znanium.com/catalog/document?id=426504#bib . | электронный ресурс |
| 5. | Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - Москва: ФОРУМ: ИНФРА-М, 2021. - 352 с. - (Среднее профессиональное образование) - https://znanium.com/read?id=364477 . | электронный ресурс |
| ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА | | |
| | Учебники, учебные пособия | |
| 1. | Баранова, Е.К. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. - Москва: РИОР: ИНФРА-М, 2022. - 202 с. - (Среднее профессиональное образование). - DOI: https://doi.org/10.29039/01806-4 . - ISBN 978-5-369-01806-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1860126 (дата обращения: 21.08.2023). | электронный ресурс |
| 2. | Ищейнов, В.Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной | электронный ресурс |

| | | |
|----|---|--------------------|
| | информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - Москва: ИНФРА-М, 2022. - 256 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1861659 (дата обращения: 21.08.2023). | |
| 3. | Петренко, В.И. Защита персональных данных в информационных системах. Практикум: учебное пособие для СПО / В.И. Петренко, И.В. Мандрица. — Санкт-Петербург: Лань, 2021. — 108 с. — ISBN 978-5-8114-6924-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/153678 (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей. | электронный ресурс |
| 4. | Прохорова, О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 124 с. — ISBN 978-5-8114-7338-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/158939 (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей. | электронный ресурс |

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в форме текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по профессиональному модулю за период обучения. Форма промежуточной аттестации – дифференцированный зачет, экзамен, экзамен (квалификационный).

Текущий контроль успеваемости осуществляется в процессе проведения практических занятий и лабораторных работ, обеспечивает оценивание хода освоения профессионального модуля.

Формы текущего контроля успеваемости: *тестирование, устный опрос, доклады, выполнение лабораторных работ.*

| № | Наименование темы (раздела) | Результаты обучения по дисциплине | Формы контроля |
|----|--|-------------------------------------|--|
| 1. | МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи. | ПК 3.1 ПК 3.2 ПК 3.3 ОК 01 | Текущий контроль педагога в форме оценки решения задач, защиты лабораторных работ. Итоговый контроль в форме экзамена (квалификационного). |
| | Тема 1. Основы безопасности информационных технологий. | ОК 02 ОК 03 ОК 04 ОК 05 | |
| | Тема 2. Обеспечение безопасности информационных технологий. | ОК 06 ОК 07 ОК 08 ОК 09 | |
| | Тема 3. Обеспечение безопасности стандартными средствами защиты. | | |
| | Тема 4. Криптографическая защита информации. | | |

Критерии оценивания результатов обучения по профессиональному модулю шкала оценивания

Критерии оценивания:

- усвоение программного теоретического материала (объем знаний, глубина усвоения);
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания на практике.

Шкала оценивания:

Результаты сдачи дифференцированного зачета, экзамена, экзамена (квалификационного) оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «зачтено» выставляется обучающемуся, который имеет знания основного материала, проявляет умение логично его излагать, хотя может допускать неточности в изложении материала, недостаточно правильные формулировки; умеет в целом применять полученные знания при выполнении типовых практических работ, хотя может испытывать затруднения при их выполнении.

Оценка «отлично» выставляется обучающемуся, который глубоко и прочно усвоил программный материал, проявляет знание основной и дополнительной литературы, грамотно, логически стройно и аргументировано излагает материал, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями.

Оценка «хорошо» выставляется обучающемуся, твердо знающему программный материал, который излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, не испытывает затруднений с ответами на вопросы.

Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на 2024-2025 учебный год по профессиональному модулю ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: в раздел Условия реализации учебной дисциплины (пункт Информационное обеспечение учебной дисциплины) внесены изменения в список основной и дополнительной литературы.

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК общетехнических дисциплин.

«30» августа 2024 г. (протокол № 1)

Председатель ПЦК  /Кузнецов Е.Ю./

Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на 2024-2025 учебный год по профессиональному модулю ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи.

В рабочую программу внесены следующие изменения:

В соответствии с приказом Минпросвещения Российской Федерации

№ 464 от 03.07.2024г. «О внесении изменений в федеральные государственные образовательные стандарты среднего профессионального образования» (утвержден Министерством юстиции Российской Федерации 09.08.2024 № 79088) изменено наименование общих компетенций дисциплины:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.

ОК 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.

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК общетехнических дисциплин.

«30» августа 2024 г. (протокол № 1)

Председатель ПЦК  /Кузнецов Е.Ю./