МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

РОСТОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ РОСТОВСКОЙ ОБЛАСТИ

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

##### РаБочая ПРОГРАММа

профессионального модуля

**ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

программы подготовки специалистов среднего звена

по специальности

**11.02.15 «Инфокоммуникационные сети и системы связи»**

(базовой подготовки)

г. Ростов-на-Дону

2022 г.

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  «Информационной безопасности»  Протокол № 1 от «31» августа 2022 г.  Председатель ЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_О.В. Копылова | **УТВЕРЖДАЮ**  Заместитель директора по НМР  \_\_\_\_\_\_\_\_\_\_\_\_\_\_И.В. Подцатова  « 31 » августа 2022 г. |

Рабочая программа профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» специальности среднего профессионального образования 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного приказом Министерства образования и науки Российской Федерации Приказ Минобрнауки России от 28.07.2014 N 811 (ред. от 21.10.2019) "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи (Зарегистрировано в Минюсте России 19.08.2014 N 33637).

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Разработчики:

МДК.03.01 «Применение программно- аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи» Копылова О.В. – преподаватель ГБПОУ РО «РКСИ»

МДК.03.02 «Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи» Копылова О.В. – преподаватель ГБПОУ РО «РКСИ»

УП 03.01 «Учебная практика» Копылова О.В. – преподаватель ГБПОУ РО «РКСИ»

Рецензенты:

Арутюнян М.М. – преподаватель ГБПОУ РО «РКСИ»

Масютин А.Н. – начальник управления системных проектов Ростовского НТЦ ФГУП «НПП «Гамма»

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| **1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** | **СТР.**  **4** |
| **2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** | **9** |
| **3. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** | **12** |
| **4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ** | **25** |
| **5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)** | **28** |

**1. паспорт РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи**

**1.1. Область применения рабочей программы**

Рабочая программа профессионального модуля ПМ. 03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» (далее ПМ) – является частью программы подготовки специалистов среднего звена по специальности 11.02.15 Инфокоммуникационные сети и системы связи базовой подготовки в части освоения основного вида профессиональной деятельности (ВПД): Обеспечение информационной безопасности инфокоммуникационных сетей и систем связии соответствующих профессиональных компетенций (ПК):

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.

В результате изучения профессионального модуля студент должен освоить вид деятельности Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи и соответствующие ему общие компетенции:

ОК1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК3 планировать и реализовывать собственное профессиональное и личностное развитие.

ОК4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ОК8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК9. Использовать информационные технологии в профессиональной деятельности.

ОК10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

Рабочая программа профессионального модуля ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи предназначена для студентов 4 курса очной формы обучения.

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи может быть использована в дополнительном профессиональном образовании в рамках реализации программ переподготовки кадров в учреждениях СПО.

В результате изучения профессионального модуля студент должен освоить вид деятельности Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи и соответствующие ему личностные результаты:

|  |  |
| --- | --- |
| **Код личностных результатов реализации программы воспитания** | **Личностные результаты**  **реализации программы воспитания**  *(дескрипторы)* |
| **ЛР 1** | Осознающий себя гражданином и защитником великой страны. |
| **ЛР 10** | Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой. |
| **ЛР 14** | Осознающий и выполняющий требования трудовой дисциплины |
| **ЛР 15** | Осознающий важность соблюдения норм законодательства и внутренней документации в отношении использования и сохранности конфиденциальной и инсайдерской информации, полученной в результате исполнения своих должностных обязанностей |
| **ЛР 25** | Демонстрирующий уровень подготовки, соответствующий современным стандартам и передовым технологиям, потребностям регионального рынка и цифровой экономики, в том числе требованиям стандартов Ворлдскиллс |
| **ЛР 26** | Способный использовать различные цифровые средства и умения, позволяющие во взаимодействии с другими людьми достигать поставленных целей в цифровой среде |
| **ЛР 27** | Стремящийся к саморазвитию и самосовершенствованию, мотивированный к обучению, принимающий активное участие в социально-значимой деятельности на местном и региональном уровнях |
| **ЛР 16** | Выполняющий требования действующего законодательства, правил и положений внутренней документации Компании в полном объеме |
| **ЛР 18** | Вовлеченный, способствующий продвижению положительной репутации Компании |
| **ЛР 21** | Осознающий принципы корпоративной социальной ответственности, соблюдающий минимальные стандарты социально ответственного поведения по отношению к пользователям информационного пространства. |
| **ЛР 22** | Не использующий сам и не способствующий использованию и дальнейшему распространению пиратского контента в сети. |

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

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения ПМ должен:

**иметь практический опыт:**

* выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности;
* разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
* осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения, и оборудования.

**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 нормативных документов 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.

Практическая подготовка реализуется на всех практических учебных занятиях профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»

**1.3. Рекомендуемое количество часов на освоение рабочей программы профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

|  |  |
| --- | --- |
| Всего | – 442 часов |
| В том числе:  - обязательную аудиторную учебную нагрузку обучающегося | – 288 часов |
| - самостоятельную работу обучающегося | – 50 часов |
| - учебная практика | – 36 часов |
| - производственная практика | – 36 часов |
| Квалификационный экзамен | – 12 часов |

# **2. Результаты освоения ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

Результатом освоения программы профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» является овладение обучающимися видом профессиональной деятельности (ВПД) разработка программных модулей программного обеспечения для компьютерных систем, в том числе профессиональными (ПК), общими компетенциями (ОК):

|  |  |
| --- | --- |
| **Код** | **Наименование результата обучения** |
| ПК 3.1 | **Практический опыт:**  - анализировать сетевую инфраструктуру;  - выявлять угрозы и уязвимости в сетевой инфраструктуре  **Умения:**  - 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.  **Знания:**  - 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. |
| ПК 3.2 | **Практический опыт:**  - разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи  **Умения:**  - определять оптимальные способы обеспечения информационной безопасности;  - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях  **Знания:**  - правила проведения возможных проверок согласно нормативных документов 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 |
| ПК 3.3 | **Практический опыт:**  - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи  - использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.  **Умения:**  - 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.  **Знания:**  - 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. |
| 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 иностранных языках. |
| ОК 11 | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере |

**3. СТРУКТУРА и содержание профессионального модуля**

**3.1. Тематический план профессионального модуля**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Код профессиональной компетенции** | **Наименования МДК профессионального модуля** | **Всего (максимальное количество), часов** | **Объем времени, отведенный на освоение  междисциплинарного курса** | | | | | **Практика** | |
| **Обязательная аудиторная учебная нагрузка обучающегося** | | | **Самостоятельная работа обучающегося** | | **Учебная,** часов | **Производ ственная(по профилю специальности и преддипломная),** часов |
| **Всего (обязательная аудиторная нагрузка),** часов | **В том числе** | | **Всего,** часов | **курсовая работа (проект),** часов |
| **лаб.работы  и практич. занятия,** часов | **курсовая работа (проект),** часов |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| ПК 3.1, 3.3  ОК 01-10  ЛР15,ЛР10 | МДК 03.01 Применение программно- аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи | 169 | 144 | 78 | - | 25 | - |  |  |
| ПК 3.1-3.3  ОК 01-10  ЛР21,ЛР22 | МДК 02.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи | 169 | 144 | 72 | - | 25 | - |  |  |
| ПК 3.1-3.3  ОК 01-10 | Учебная практика |  |  |  |  |  |  | 36 |  |
| ПК 3.1-3.3  ОК 01-10 | Производственная практика (по профилю специальности) |  |  |  |  |  |  |  | 36 |
| **Всего:** | | **338** | **288** | **150** | **-** | **50** | **-** | **36** | **36** |

# **3.2. Содержание обучения по профессиональному модулю**

| **Наименование разделов и тем** | | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся** | | **Объем часов** | **Уровень освоения** | |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | | 2 | | 3 | 4 | |
| **МДК.03.01 Применение программно- аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи** | | | | **144** |  | |
| **Тема 1.1.**Основы безопасности информационных технологий | | **Содержание учебного материала** | | **14** | ПК 3.1, 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий. | 2 |
|  | Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность. | 2 |
|  | Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности | 2 |
|  | Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе. | 2 |
|  | Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры. | 2 |
|  | Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. | 2 |
|  | Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности. | 2 |
| **Практические занятия** | | **12** |
|  | **Практическое занятие №1**. Определение выполняемых процессов. Изучение процессов, потоков, дескрипторов и реестра Windows. Создание учетных записей пользователей | 2 |
|  | **Практическое занятие №2**. Создание учетных записей пользователей. Использование Windows PowerShell. | 2 |
|  | **Практическое занятие №3.** Диспетчер задач Windows. Мониторинг системных ресурсов в Windows и управление ими. | 2 |
|  | **Практическое занятие №4.** Использование командной строки Linux. Основные команды. | 2 |
|  | **Практическое занятие №5.** Службы Linux. Журналы Linux. | 2 |
|  | **Практическое занятие №6.** Файловая система. Управление правами доступа | 2 |
| **Тема 1.2.** Обеспечение безопасности информационных технологий | | **Содержание учебного материала** | | **20** | ПК 3.1, 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ. | 2 |
|  | Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации. | 2 |
|  | Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты. | 2 |
|  | Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедур авторизации сотрудников. | 2 |
|  | Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация. | 2 |
|  | Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем. | 2 |
|  | Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов. | 2 |
|  | Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы. | 2 |
|  | Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации. | 2 |
|  | Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции. | 2 |
| **Практические занятия** | | **16** |
|  | **Практическое занятие №7**. Установка и настройка антивирусного ПО | 2 |
|  | **Практическое занятие №8.** Создание дискреционной модели безопасности. Создание скрытой информации. Установка паролей | 2 |
|  | **Практическое занятие №9**. Разграничение прав доступа для пользователей локального  компьютера и локальной сетиWindows | 2 |
|  | **Практическое занятие №10.** Настройка параметров политики аудита | 2 |
|  | **Практическое занятие №11.** Настройка параметров политики безопасности операционной системы Windows | 2 |
|  | **Практическое занятие №12.** Архивация и восстановление данных Windows | 2 |
|  | **Практическое занятие №13** Предотвращение и исправление ошибок жесткого диска CrystalDiskInfo | 2 |
|  | **Практическое занятие №14.** Защитные механизмы в приложениях (на примере MSWord, MSExcel, MSPowerPoint) | 2 |
| **Тема 1.3.** Средства защиты информации от несанкционированного доступа | | **Содержание учебного материала** | | **18** | ПК 3.1, 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов | 2 |
|  | Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации. | 2 |
|  | Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOСK) | 2 |
|  | Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть».) | 2 |
|  | Назначение и особенности применения СЗИ НСД (например, «Страж NT») | 2 |
|  | Назначение и специфика применения комплекса ЗИ (например, «Соболь») | 2 |
|  | Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей. | 2 |
|  | Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана. | 2 |
|  | Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа.  Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности | 2 |
| **Практические занятия** | | **18** |
|  | **Практическое занятие 15** Установка и запуск программы OpenSSL в ОС Windows. Основы работы в OpenSSL | 2 |
|  | **Практическое занятие 16** Использование алгоритмов шифрования для сокрытия содержимого файла с применением OpenSSL | 2 |
|  | **Практическое занятие 17** Использование алгоритмов хеширования для подтверждения неизменности файла с применением OpenSSL | 2 |
|  | **Практическое занятие 18** Создание цифровых сертификатов Х.509 и преобразование их форматов с применением пакета OpenSSL | 2 |
|  | **Практическое занятие 19** Создание центра сертификации с поддержкой списков отозванных сертификатов с применением пакета OpenSSL | 2 |
|  | **Практическое занятие 20** Применение «сетей доверия» для распространения сертификатов | 2 |
|  | **Практическое занятие 21** Применение электронной цифровой подписи для проверки авторства и неизменности файла | 2 |
|  | **Практическое занятие № 22** Создание сертификатов и ключей для OpenVPN сервера и клиента. | 2 |
|  | **Практическое занятие № 23** Создание файлов конфигурации OpenVPN сервера и клиентов**.** | 2 |
| **Тема 1.4.** Обеспечение безопасности компьютерных систем и сетей | | **Содержание учебного материала** | | **12** | ПК 3.1, 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация. | 2 |
|  | Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов. | 2 |
|  | Анализ содержимого почтового и WEB-трафика. HTTP-трафик. | 2 |
|  | Виртуальные частные сети. Решение на базе ОС Windows Server 2019. VPN на основе криптошлюза (например, «Континент-К») | 2 |
|  | Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности. | 2 |
|  | Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак. | 2 |
| **Практические занятия** | | **32** |
|  | **Практическое занятие № 24** Установка SNS, настройка политик безопасности. Настройка полномочного управления доступом SNS | 2 |
|  | **Практическое занятие № 25** Настройка аудита операционной системы и событий SNS. Работа с журналом событий. Настройка механизма дискреционного управления доступом | 2 |
|  | **Практическое занятие № 26** Управление доступом к съемным носителям информации | 2 |
|  | **Практическое занятие № 27** Настройка механизма замкнутой программной среды SNS | 2 |
|  | **Практическое занятие № 28** Настройка механизма контроля целостности | 2 |
|  | **Практическое занятие №29**. Настройка стенда для SN LSP | 2 |
|  | **Практическое занятие № 30.** Управление учетными записями пользователей с помощью Secret Net LSP | 2 |
|  | **Практическое занятие № 31.** Настройка параметров работы Secret Net LSP | 2 |
|  | **Практическое занятие № 32.** Настройка механизма контроля целостности | 2 |
|  | **Практическое занятие № 33**. Настройка механизма дискреционного управления доступом | 2 |
|  | **Практическое занятие № 34.** Управление доступом к съемным носителям информации | 2 |
|  | **Практическое занятие № 35.** Настройка механизма замкнутой программной среды | 2 |
|  | **Практическое занятие № 36.** Настройка персонального межсетевого экрана | 2 |
|  | **Практическое занятие № 37.** Построение закрытого контура | 2 |
|  | **Практическое занятие № 38.** Установка и настройка антивирусного ПО | 2 |
|  | **Практическое занятие № 39.** Архивация и восстановление данных.Резервное копирование | 2 |
| Дифференцированный зачет | | | | **2** |  | |
| **Самостоятельная работа при изучении МДК03.01.**  - Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы.  - Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.  - Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.  - Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.  **Рекомендуемая тематика внеаудиторной самостоятельной работы:**  1. Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре.  2. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа.  3. Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.  4. Применение различных программ для оперативного и гарантированного восстановления информации на ПК.  5. Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации.  6. Разработка комплекса организационно-административной защиты от вредоносных программ.  7. Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте.  8. Применение подсистемы безопасности WINDOWS 10 для предотвращения несанкционированного доступа к защищаемой информации. | | | | **25** | ПК 3.1, 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
| **МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи** | | | |  |  | |
| **Тема 2.1.** Основы информационной безопасности | | **Содержание учебного материала** | | **12** | ПК 3.1- 3.3  ОК 01-10 | |
|  | Основные понятия информационной безопасности. Сущность и понятия защиты информации | 2 |
|  | Значение информационной безопасности и ее место в системе национальной безопасности. | 2 |
|  | Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере. | 2 |
|  | Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. | 2 |
|  | Состояние информационной безопасности РФ и основные задачи по ее обеспечению. | 2 |
|  | Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности | 2 |
| **Тема 2.2.** Организационно-правовые аспекты защиты информации | | **Содержание учебного материала** | | **10** | ПК 3.1- 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Структура правовой защиты информации. Система документов в области защиты информации. | 2 |
|  | Организационные основы защиты информации. Принципы организационной защиты информации. | 2 |
|  | Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации. | 2 |
|  | Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности. | 2 |
|  | Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере. | 2 |
| **Тема 2.3.** Комплексная система защиты информации | | **Содержание учебного материала** | | **12** | ПК 3.1- 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации | 2 |
|  | Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна. | 2 |
|  | Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны. | 2 |
|  | Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение. | 2 |
|  | Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз. | 2 |
|  | Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна. | 2 |
| **Практические занятия** | | **46** |
|  | **Практическое занятие 1.** Определение целей и задач защиты информации на исследуемом объекте, основных объектов защиты, предмет защиты. | 2 |
|  | **Практическое занятие 2.** Определение факторов, влияющих на защиту информации на исследуемом объекте, выявление возможных угроз защищаемой информации и их структуру | 2 |
|  | **Практическое занятие 3.** Исследование уязвимостей и построение модели угроз объекта защиты. |  |
|  | **Практическое занятие 4.** Выявление источников, видов и способов дестабилизирующего воздействия на защищаемую информацию на исследуемом объекте, выявление причин их дестабилизирующего воздействия | 2 |
|  | **Практическое занятие 5.** Выявление каналов и методов несанкционированного доступа к защищаемой информации на исследуемом объекте. | 2 |
|  | **Практическое занятие 6.** Выявление и оценка свойств каналов утечки информации | 2 |
|  | **Практическое занятие 7.** Разработка комплексной системы инженерно-технической защиты информации на объекте. |  |
|  | **Практическое занятие 8.** Определение основных направлений, методов и средств защиты информации | 2 |
|  | **Практическое занятие 9.** Разработка методов защиты объекта | 2 |
|  | **Практическое занятие 10.** Описание основных методов и средств инженерной защиты, выбранных для защиты объекта | 2 |
|  | **Практическое занятие 11.** Описание места расположения и требуемые параметры средств инженерной защиты | 2 |
|  | **Практическое занятие 12.** Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств | 2 |
|  | **Практическое занятие 13.** Виды штрих-кодов, их генерация и считывание | 2 |
|  | **Практическое занятие 14.** Построение системы контроля управления доступом (СКУД) на базе контактных смарт-карт | 2 |
|  | **Практическое занятие 15.** Построение СКУД на базе бесконтактных RFID смарт-карт | 2 |
|  | **Практическое занятие 16.** Построение СКУД на базе биометрических систем | 2 |
|  | **Практическое занятие 17.** Построение СКУД на базе ключей eToken | 2 |
|  | **Практическое занятие 18**. Построение домофонной системы | 2 |
|  | **Практическое занятие 19**. Система аутентификации на основе цифровых сертификатов. | 2 |
|  | **Практическое занятие 20.** Настройка и работа с сервером RADIUS. | 2 |
|  | **Практическое занятие 21**. Использование протокола 802.1X для авторизации пользователей сети. | 2 |
|  | **Практическое занятие 22**. Виды штрих-кодов, их генерация и считывание | 2 |
|  | **Практическое занятие 23**. Построение системы контроля управления доступом (СКУД) на базе контактных смарт-карт | 2 |
| **Тема 2.4.** Инженерно-техническая защита информации | | **Содержание учебного материала** | | **26** | ПК 3.1- 3.3  ОК 01-10 | |
|  | Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты. | 2 |
|  | Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации. | 2 |
|  | Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации. | 2 |
|  | Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации. | 2 |
|  | Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД. | 2 |
|  | Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению. | 2 |
|  | Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи. | 2 |
|  | Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания. | 2 |
|  | Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок | 2 |
|  | Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания. | 2 |
|  | Контроль слаботочных цепей. Принципы контроля линий заземления. | 2 |
|  | Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации. | 2 |
|  | Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники. | 2 |
| **Практические занятия** | | **26** |
|  | **Практическое занятие 24.** Селективный индикатор поля RAKSA-120 | 2 |
|  | **Практическое занятие 25.** ST 131 ПИРАНЬЯ-II многофункциональное поисковое устройство каналов утечки информации | 2 |  | |
|  | **Практическое занятие 26.** Универсальный поисковый прибор D 008 | 2 |
|  | **Практическое занятие 27.** ЛОРНЕТ 24 нелинейный локатор | 2 |
|  | **Практическое занятие 28.** Обнаружитель видеокамер "АРКАМ" С-200. "Алмаз". Оптик-2 | 2 |
|  | **Практическое занятие 29** Магнитный томограф Дозор1 | 2 |
|  | **Практическое занятие 30.** Шумогенератор "Гром-ЗИ-4" | 2 |
|  | **Практическое занятие 31.** Блокиратор сотовой связи ЛГШ-719 | 2 |
|  | **Практическое занятие 32.** Генератор радиошума переносной ПРП-2500 | 2 |
|  | **Практическое занятие 33.** Подавитель диктофонов "Барсетка" | 2 |
|  | **Практическое занятие 34.** Подавитель диктофонов Завеса-Аудио Максимум 7 | 2 |
|  | **Практическое занятие 35.** Система виброакустической защиты "Соната-АВ-1М" | 2 |
|  | **Практическое занятие 36.** Обнаружение каналов утечки речевой информации | 2 |
| **Тема 2.5.** Криптографическая защита информации | | **Содержание учебного материала** | | **8** | ПК 3.1- 3.3  ОК 01-10  ЛР10,ЛР15,ЛР21 | |
|  | Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных. | 2 |
|  | 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. | 2 |
| **Практические занятия** | |  |
| **Тема 2.5.** Аттестация и лицензирование объектов защиты | | **Содержание учебного материала** | | **6** | ПК 3.1- 3.3  ОК 01-10 | |
|  | Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ. | 2 |
|  | Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний | 2 |
|  | Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании | 2 |
| Дифференцированный зачет | | | | **2** |  |
| Самостоятельная работа при изучении МДК.03.02:  - изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере;  - ознакомление с нормативными документами по ИБ;  - изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности;  - составление доклада по перспективным направлениям развития средств комплексной защиты информации;  - разработка пакета документации по инженерно-технической защите информации на объекте;  - изучение возможностей инженерно-технических средств защиты информации;  - изучение технических характеристик инженерно-технических средств защиты информации;  - разработка предложений по инженерно-технической защите информации на определенном объекте; | | | |  | ПК 3.1-3.3  ОК 01-10 |
| **Учебная практика** | | | | **36** | ПК 3.1-3.3  ОК 01-10 |
| **Тема 2.1.** Инженерно-технические средства защиты информации |  | | Практическое занятие 1. Описание объекта информатизации. | 2 |
|  | | Практическое занятие 2. Построение модели нарушителя. | 2 |
|  | | Практическое занятие 3. Изучение проекта типового комплекса инженерно-технических средств физической защиты | 2 |
|  | | Практическое занятие 4. Оценка уязвимости объектов комплекса инженерно-технических средств физической защиты | 2 |
|  | | Практическое занятие 5. Изучение типового проекта системы охранной сигнализации | 2 |
|  | | Практическое занятие 6. Оценка уязвимости объектов системы охранной сигнализации | 2 |
|  | | Практическое занятие 7. Изучение типового проекта системы пожарной сигнализации | 2 |
|  | | Практическое занятие 8. Оценка уязвимости объектов системы пожарной сигнализации | 2 |
|  | | Практическое занятие 9. Изучение типового проекта системы контроля и управления доступом | 2 |
|  | | Практическое занятие 10. Оценка уязвимости объектов системы контроля и управления доступом | 2 |
|  | | Практическое занятие 11. Изучение типового проекта системы аналогового видеонаблюдения | 2 |
|  | | Практическое занятие 12. Изучение типового проекта системы цифрового видеонаблюдения | 2 |
|  | | Практическое занятие 13. Оценка уязвимости объектов системы видеонаблюдения | 2 |
|  | | Практическое занятие 14. Изучение типового проекта системы сбора, обработки, отображения и документирования информации | 2 |
|  | | Практическое занятие 15. Оценка уязвимости объектов системы сбора, обработки, отображения и документирования информации | 2 |
|  | | Практическое занятие 16. Изучение типового проекта системы воздействия | 2 |
|  | | Практическое занятие 17. Оценка уязвимости объектов системы воздействия | 2 |
|  | | Практическое занятие 18. Изучение типового проекта системы умного дома и оценка уязвимости объектов системы умного дома | 2 |
| 1. Производственная практика (по профилю специальности) по ПМ 2. Виды работ: 3. Участие в создании комплексной системы защиты на предприятии 4. Применение программно-аппаратных средств защиты информации на предприятии 5. Применение инженерно-технических средств защиты информации на предприятии. 6. Применение криптографических средств защиты информации на предприятии. 7. Принятие участия в выявлении технических каналов утечки информации; 8. Участие в техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, инженерно-технических средств физической защиты и технических средств защиты информации 9. Участие в установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; 10. Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; 11. Проведение и измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. 12. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 13. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 14. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 15. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. | | | | **36** | ПК 3.1-3.3  ОК 01-10 |
| **Промежуточная аттестация (экзамен)** | | | | **12** |  |
| **Всего** | | | | **422** |  |

# **4. условия реализации программы профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

# **4.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы профессионального модуля требует наличия

* учебных кабинетов, лабораторий:
* Лаборатория «Информационной безопасности телекоммуникационных систем».

Лаборатория «Информационной безопасности телекоммуникационных систем».должна быть оснащена:

* антивирусными программными комплексами;
* аппаратными средствами аутентификации пользователя;
* программно-аппаратными средствами управления доступом к данным и защиты (шифрования) информации;
* средствами защиты информации от НСД, блокирования доступа и нарушения целостности;
* программными средствами криптографической защиты информации;
* программными средствами выявления уязвимостей и оценки защищенности ИТКС,
* анализа сетевого трафика;
* системы разграничения доступа;
* межсетевые экраны;
* средство криптографической защиты информации, реализующее функции удостоверяющего центра и создания виртуальных сетей;
* комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).
* средствами защиты информации от утечки по акустическому (виброакустическому) каналу;
* средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок;
* средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок.

Реализация рабочей программы профессионального модуля предполагает наличие учебной и производственной (по профилю специальности) практики, которые проводятся концентрированно.

# **4.2. Информационное обеспечение обучения. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

Рекомендуемая литература:

*Основные источники (название учебников, размещенных в библиотеке колледжа, учебные пособия, разработанные преподавателем, в том числе* *и в форме электронных конспектов*)*:*

1. [Зайцев А.П.,](http://www.techbook.ru/book_list.php?str_author=Зайцев%20А.П.)[Мещеряков Р.В.,](http://www.techbook.ru/book_list.php?str_author=Мещеряков%20Р.В.)[Шелупанов А.А.](http://www.techbook.ru/book_list.php?str_author=Шелупанов%20А.А.) Технические средства и методы защиты информации. 7-е изд., испр. – М.: «Горячая линия» - Телеком, 2020. –444стр.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: «Горячая линия» - Телеком, 2020 – 586 стр.
4. Бузов Г. А.Выявление специальных технических средств несанкционированного получения информации. - М.: «Горячая линия» - Телеком, 2020 – 203 стр.
5. Карпухин Е.О. Технологии и методы защиты инфокоммуникационных систем и сетей. - М.: «Горячая линия» - Телеком, 2020 – 120 стр.
6. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками . - М.: «Горячая линия» - Телеком, 2020 – 352стр.
7. Шива Парарасрам, Алекс Замм, Kali Linux Тестирование на проникновение и безопасность. Изд. Питер, 2020, 441 стр.
8. А.П. Душкин. Программно-аппаратные средства обеспечения информационной безопасности. Изд.: Москва Горячая линия- Телеком, 2020, 242мтр.
9. А.О. Чефранова, Технология построения VPN VipNet: курс лекций. Тзд.: Москва Горячая линия – Телекос, 2018. 334 стр.
10. Букатов Александр Алексеевич, Гуда Сергей Александрович. Компьютерные сети. Расширенный начальный курс. Спб. : Питер, 2019.
11. .Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы : Учеб. пособие для вузов / В. Г. Олифер, Н.А. Олифер. Спб. : Питер, 2019.
12. Таненбаум, Э. Компьютерные сети/ Э. Таненбаум, Д. Уэзеролл– 5-е изд. – Спб.: Питер, 2017.
13. Куроуз, Дж.Компьютерные сети: Нисходящий подход / Дж. Куроуз; К.Росс. – М.: Э, 2016.
14. Л.Г. Гагарина. Разработка и эксплуатация автоматизированных информационных систем. ИД Форум 2021, 384 стр.
15. В.Б. Кравченко, П.В. Зиновьев, И.Н. Селютин. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. ИЦ «Академия» 2018, 299 стр.
16. Таненбаум Эндрю, Бос Х. Современные операционные системы. Изд. – Спб.: Питер, 2018, 1120 стр.
17. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2014.
18. Костров Б. В. , Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2016.
19. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 2-е изд.- М.: Горячая линия-Телеком, 2014.
20. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2013.
21. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

*Дополнительные источники:*

*Интернет–ресурсы:*

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
5. <http://www.morion.ru/>
6. <http://www.nateks.ru/>
7. <http://www.iskratel.com/>
8. <http://www.ps-ufa.ru/>
9. <http://3m.com/>
10. <http://www.rusgates.ru/index/php> - Материалы сайта завода «Ферроприбор»
11. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
12. Информационный портал по безопасности www.SecurityLab.ru.
13. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
14. Российский биометрический портал www.biometrics.ru
15. Сайт журнала Информационная безопасность http://www.itsec.ru –
16. Сайт Научной электронной библиотеки www.elibrary.ru
17. Справочно-правовая система «Гарант» » www.garant.ru
18. Справочно-правовая система «Консультант Плюс» www.consultant.ru
19. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
20. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
21. Федеральный портал «Российское образование www.edu.ru

# **4.3. Общие требования к организации образовательного процесса**

Перед изучением профессионального модуля обучающиеся изучают следующие учебные дисциплины:

* Информатика и ИКТ;
* Информационные технологии;
* Основы программирования;
* Операционные системы.

**4.4 Кадровое обеспечение образовательного процесса**

1. Квалификация педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарным курсам:

МДК.03.01. – Копылова О.В. – преподаватель ГБПОУ РО «РКСИ»

МДК.03.02. – Бороненкова С.Е.. – преподаватель ГБПОУ РО «РКСИ»

1. Квалификация педагогических (инженерно-педагогических) кадров, осуществляющих руководство практикой:

УП.03.01. – Азарова Н.И. – преподаватель ГБПОУ РО «РКСИ»

ПП.01.01. – \_\_\_\_\_\_\_\_\_\_ – преподаватель ГБПОУ РО «РКСИ»

Образование педагогических работников соответствует профилю преподаваемого профессионального модуля, а повышение квалификации - требованиям ФГОС СПО.

**5. Контроль и оценка результатов освоения ПМ**

Организация и порядок текущего контроля и промежуточной аттестации регулируются локальным «Положением о текущем контроле и промежуточной аттестации студентов ГБПОУ РО «РКСИ».

|  |  |  |
| --- | --- | --- |
| **Результаты обучения**  **(освоенные профессиональные компетенции)** | **Основные показатели оценки результатов обучения** | **Формы, методы контроля и оценки результатов обучения** |
| ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности | классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно;  анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный;  возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно;  мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме;  недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме,  тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно; | тестирование,  экзамен,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |
| ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. | для обеспечения информационной безопасности выбраны оптимальные способы;  выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях; | тестирование,  экзамен,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |
| ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования | мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными;  политика безопасности сетевых элементов и логических сетей разработана в полном объеме;  расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами;  установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами;  конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами;  базы данных максимально защищены при помощи специализированных программных продуктов;  ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами; | тестирование,  экзамен,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |

|  |  |  |
| --- | --- | --- |
| **Результаты обучения**  **(освоенные общие компетенции и личностные результаты)** | **Основные показатели оценки результатов обучения** | **Формы и методы контроля и оценки результатов обучения** |
| ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;  адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы  Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам  Экзамен |
| ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | демонстрация ответственности за принятые решения  обоснованность самоанализа и коррекция результатов собственной работы; |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;  обоснованность анализа работы членов команды (подчиненных) |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | грамотность устной и письменной речи,  ясность формулирования и изложения мыслей |
| ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения | соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;  знание и использование ресурсосберегающих технологий в области телекоммуникаций |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. | эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; |
| ОК 09. Использовать информационные технологии в профессиональной деятельности | эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке | эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке |
| ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере | эффективность использования знаний по финансовой грамотности, планирования предпринимательскую деятельность в профессиональной сфере |
| ЛР 1 Осознающий себя гражданином и защитником великой страны | соблюдение этических норм общения при взаимодействии с обучающимися, преподавателями, мастерами и руководителями практики | анализ соблюдения норм и правил поведения, принятых в колледже, обществе, профессиональном сообществе;  анализ самооценки событий обучающимися;  педагогический и психологический мониторинг;  анализ проявления обучающимися качеств своей личности: оценка поступков, осознание своей жизненной позиции, культурного выбора, мотивов личностных целей |
| ЛР 10 Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой | отсутствие социальных конфликтов среди обучающихся, основанных на межнациональной, межрелигиозной почве |
| ЛР 14 Осознающий и выполняющий требования трудовой дисциплины | участие в конкурсах профессионального мастерства, олимпиадах по профессии, викторинах, в предметных неделях;  участие в исследовательской и проектной работе;  участие в конкурсах профессионального мастерства и в командных проектах | мониторинг роста творческой самостоятельности и навыков получения нового знания обучающимися  экспертная оценка деятельности;  анализ участия в проектах, конкурсах профессионального мастерства, предметных олимпиадах, проектах, выполнения творческих заданий |
| ЛР 15 Осознающий важность соблюдения норм законодательства и внутренней документации в отношении использования и сохранности конфиденциальной и инсайдерской информации, полученной в результате исполнения своих должностных обязанностей |
| ЛР 16 Выполняющий требования действующего законодательства, правил и положений внутренней документации Компании в полном объеме |
| ЛР 18 Вовлеченный, способствующий продвижению положительной репутации Компании |
| ЛР 21 Осознающий принципы корпоративной социальной ответственности, соблюдающий минимальные стандарты социально ответственного поведения по отношению к пользователям информационного пространства | проявление культуры потребления информации, умений и навыков пользования компьютерной техникой, навыков отбора и критического анализа информации, умения ориентироваться в информационном пространстве | анализ продуктов деятельности (проектов, практических, творческих работ);  экспертная оценка;  наблюдение |
| ЛР 22 Не использующий сам и не способствующий использованию и дальнейшему распространению пиратского контента в сети |
| ЛР 25 Демонстрирующий уровень подготовки, соответствующий современным стандартам и передовым технологиям, потребностям регионального рынка и цифровой экономики, в том числе требованиям стандартов Ворлдскиллс |
| ЛР 26 Способный использовать различные цифровые средства и умения, позволяющие во взаимодействии с другими людьми достигать поставленных целей в цифровой среде |
| ЛР 27 Стремящийся к саморазвитию и самосовершенствованию, мотивированный к обучению, принимающий активное участие в социально-значимой деятельности на местном и региональном уровнях |

Лист согласования

**Дополнения и изменения к рабочей программе ПМ на учебный год**

Дополнения и изменения **к рабочей программе ПМ** на \_\_\_\_\_\_\_\_\_\_ учебный год по дисциплине Наименование\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**В рабочую программу ПМ** внесены следующие изменения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дополнения и изменения в **рабочей программе ПМ** обсуждены на заседании ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_г.

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_