**Министерство образования и науки Забайкальского края   
Государственное профессиональное образовательное учреждение «ЧИТИНСКИЙ ТЕХНИКУМ ОТРАСЛЕВЫХ ТЕХНОЛОГИЙ И БИЗНЕСА» (ГПОУ «ЧТОТиБ»)**

|  |  |  |
| --- | --- | --- |
|  |  | **УТВЕРЖДАЮ** Заместитель директора по УПП  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В Лончаков  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2021г.  М.П. |

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ**

**УП. 03.01Выполнение работ по обеспечению информационной безопасности**

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

по специальности

**11.02.15 Инфокоммуникационные сети и системы связи**

Форма обучения: очная

Курс (семестр): V(10)

2021 г.

|  |  |
| --- | --- |
| Программа учебной практики разработана на основе документов: | ФГОС СПО **11.02.15 Инфокоммуникационные сети и системы связи.** |
| Рабочей программы **ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи.** |
| Положение о практике обучающихся, осваивающих основные профессиональные образовательные программы среднего профессионального образования, утвержденное приказом Министерства образования и науки Российской Федерации 09 декабря 2016 № 1584. |
| Организация-разработчик | ГПОУ «Читинский техникум отраслевых технологий и бизнеса» |
| Автор | А.В. Горбунов |
| Рассмотрена и одобрена на заседании ПЦК № 4 | Председатель ПЦК№\_\_\_\_\_\_\_\_ /И.И. Семченкова  «\_\_»\_\_\_\_\_\_\_ 2021г. |
| Допущена | Зам. директора по научно-методической работе \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ж.В.Терукова  «\_\_»\_\_\_\_\_\_\_ 2021г. |

# **СОДЕРЖАНИЕ**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Разделы** | **стр.** |
| **1** | **ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ учебной практики** | **4** |
| **2** | **СТРУКТУРА и содержание учебной практики** | **7** |
| **3** | **условия реализации программы учебной практики** | **10** |
| **4** | **Контроль и оценка результатов Освоения учебной практики** | **14** |

# **1. ОБЩАЯ ХАРАКТЕРИСТИКАПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

* 1. **Область применения программы**

Программа профессионального модуля (далее рабочая программа) –является частью основной образовательной программы по специальности среднего профессионального обучения 11.02.15 Инфокоммуникационные сети и системы связи в соответствии с ФГОС СПО 11.02.15 Инфокоммуникационные сети и системы связи, утверждённым приказом Министерства образования и науки Российской Федерации 09 декабря 2016 № 1584.

**1.2.Цели и задачи учебной практики – требования к результатам освоения учебной практики:**

Учебная практика выполнение работ по обеспечению информационной безопасности направлена на формирование у обучающихся **умений**:

**У1.**классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

**У2.**проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;

**У3.**определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;

**У4.**осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

**У5.**выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выполнять тестирование систем с целью определения уровня защищенности;

**У6.**определять оптимальные способы обеспечения информационной безопасности;

**У7.**проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;

**У8.**проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;

**У9.**разрабатывать политику безопасности сетевых элементов и логических сетей;

**У10.**выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;

**У11.**производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;

**У12.**конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

**У13.**защищать базы данных при помощи специализированных программных продуктов;

**У14.**защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.

Приобретение **первоначальногопрактического опыта**:

**ПО1.** выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности;

**ПО2.**разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;

**ПО3.**осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения, и оборудования;

**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;

**ПК3.3**. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования;

а также**общих компетенций (ОК):**

**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 общечеловеческих ценностей;

**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 поддержание необходимого уровня физической подготовленности;

**1.3. Количество часов на освоение программы учебной практики:**объем образовательной программы - **72** часа.

**1.4.Планирование и организация практики**

* + 1. Общие требования к организации образовательного процесса

Организация практики включает три этапа:

1. Подготовительный, который предусматривает подготовку и актуализацию и дидактических материалов для проведения практических работ;
2. Текущая работа, осуществляемая в период учебной практики студентов;
3. Этап подведения итогов учебной практики.

Учебная практика проводится в ходе освоения студентами МДК 03.01, МДК 03.02.

Учебная практика проводится вучебной лаборатории «Сборка, монтаж и эксплуатация средств вычислительной техники».

Продолжительность практики для обучающихся не более 36 часов в неделю.

Учебная практика Выполнение работ по обеспечению информационной безопасностипроводится в виде практических занятий, на которых студенты выполняют, а преподаватель оценивает практические работы. Практика завершается дифференцированным зачетом в соответствии с Положением о промежуточной аттестации студентов ГПОУ ЧТОТиБ.

1.4.2 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, осуществляющих руководство учебной практикой:

Организацию и руководство практикой осуществляют преподаватели, имеющие среднее профессиональное образование, преподаватели с высшим образованием, соответствующим профилю практики.

Преподавателидолжны проходить повышение квалификации, в том числе в виде стажировки в профильных организациях не реже одного раза в три года.

**2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ**

**2.1. Объем учебной практики и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | **Количество**  **часов** |
| Учебная практика, всего | **72** |
| в том числе: |  |
| Выполнение практических работ  Виды работ:   * Криптографические алгоритмы шифрования; * Электронно-цифровая подпись; * Программно-аппаратные средства защиты информации; * Программный комплекс ViPNet Administrator; * Настройка и конфигурирование VPN-туннелей; * Межсетевые экраны. Состав программного обеспечения ViPNet OFFICE Firewall. |
| Промежуточная аттестация в форме дифференцированного зачета | |  |

# **2.2. Тематический план и содержание учебной практики«Выполнение работ по обеспечению информационной безопасности»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Разделы (этапы) учебной практики** | **Виды учебной деятельности на учебной практике, включая самостоятельную работу обучающихся (в часах)** | | **Объем часов** | **Формируемые ПК, ОК** |
| **1** | **2** | | **3** | **4** |
| **Тема 1.** Криптографические алгоритмы шифрования | **Содержание** | | 12 | **ПК 1.3**  **ОК 1-ОК 8** |
| 1 | Изучение основных симметричных и ассиметричных криптоалгоритмов шифрования. |
| **Практические занятия** | |
| 2 | **Практическая работа 1.** Симметричные и ассиметричные криптоалгоритмы шифрования. |
| **Тема 2.** Электронно-цифровая подпись | 1 | Создание и проверка цифровой электронной подписи. | 12 | **ПК 1.1, ПК 1.3**  **ОК 1, ОК 2,**  **ОК 4** |
| **Практические занятия** | |
| 2 | **Практическая работа 2.** Практическое применение ViPNet Crypto Service. |
| **Тема 3.** Программно-аппаратные средства защиты информации | 1 | Изучение основных программно-аппаратных средств защиты информации. | 12 | **ПК 1.1, ПК 1.3**  **ОК 1, ОК 2,**  **ОК 4** |
| **Практические занятия** | |
| 2 | **Практическая работа 3.** Построение систем антивирусной защиты телекоммуникационных систем и сетей. |
| **Тема 4.** Программный комплекс ViPNet Administrator | 1 | Изучение программного комплекса ViPNet Administrator (Центр управления сетью, Удостоверяющий и ключевой центр). | 12 | **ПК 1.2**  **ОК 1, ОК 3,**  **ОК 7, ОК 8** |
| **Практические занятия** | |
| 2 | **Практическая работа 4.** Изучение программного комплекса ViPNet Administrator. |
| **Тема 5.** Настройка и конфигурирование VPN-туннелей | 1 | Настройка и конфигурирование VPN-туннелей. | 12 | **ПК 1.1, ПК 1.3**  **ОК 1, ОК 2,**  **ОК 4** |
| **Практические занятия** | |
| 2 | **Практическая работа 5. Перви**чная конфигурация сети ViPNet. |
| **Тема 6.** Межсетевые экраны. Состав программного обеспечения ViPNet OFFICE Firewall. | 1 | Изучение программного обеспечения ViPNet OFFICE Firewall. | 12 | **ПК 1.1, ПК 1.3**  **ОК 1, ОК 2,**  **ОК 4** |
| **Практические занятия** | |
| 2 | **Практическая работа 6.** Межсетевые экраны. Настройка сетевых фильтров |
| **Всего:** | | **72** |  |

# **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ**

**3.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы учебной практики предполагает наличие учебных лаборатории «Сборка, монтаж и эксплуатация средств вычислительной техники».

**Оснащение учебной мастерской:**

1. рабочее место преподавателя.
2. посадочные места по количеству обучающихся.
3. персональные компьютеры;
4. простой набор инструментов для разборки и сборки;
5. диагностические устройства и программы для тестирования компонентов компьютера;
6. приборы для измерения напряжения и сопротивления, такие как цифровой мультиметр, логические пробники и генераторы одиночных импульсов для проверки цифровых схем;
7. электромонтажные столы
8. электромонтажные стенды,
9. химические препараты (раствор для протирания контактов), пульверизатор с охлаждающей жидкостью и баллончик со сжатым газом (воздухом) для чистки деталей компьютера;
10. набор тампонов для протирания контактов;
11. специализированные подручные инструменты (например, инструменты, необходимые для замены микросхем (чипов));
12. тестовые разъемы для проверки последовательных и параллельных портов;

**3.2. Информационное обеспечение обучения**

**Перечень рекомендуемых учебных изданий, дополнительной литературы**

**Основные источники:**

**Учебники:**

1. Быховский М.А. Развитие телекоммуникаций. На пути к информационному обществу. Развитие радиолокационных систем: Учебное пособие для вузов/М.А.Быховский - М.: Гор. Линия Телеком, 2019. - 402 с.: 60x88 1/16 (Обложка) ISBN 978-5-9912-0466-8.
2. Вартанян А. А. Интеллектуальные системы и инфокоммуникационные технологии на предприятиях связи. — М.: ООО " ИД Медиа Паблишер" Москва, 2019. — С. 180.
3. Гольдштейн Б.С., Елагин В.С., Сенченко Ю.Л. Протоколы ААА: RADIUS и Diameter. Серия «Телекоммуникационные протоколы». Книга 9. – СПб.БХВ – Санкт-Петербург, 2020. ISBN: 978-5-9775-0668-7
4. Рязанова Л.Е. Удовиченко О.Н. Построение сетей передачи данных. Учебное пособие. – г. Москва УМЦ СПО ФАС, 2019

# **Контроль и оценка результатов освоения учебной практики**

В результате освоения учебной практики, обучающиеся проходят промежуточную аттестацию в форме дифференцированного зачета. Оценка вычисляется как средняя по результатам выполнения всех практических работ. Оценку практических работ осуществляет руководитель практики. Оценка по каждой практической работе заносится в учебный журнал.

|  |  |
| --- | --- |
| **Результаты обучения** | **Формы и методы контроля и оценки результатов обучения** |
| **должен уметь:** |  |
| **У1.** классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;  **У2.** проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;  **У3.** определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;  **У4.** осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;  **У5.** выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выполнять тестирование систем с целью определения уровня защищенности;  **У6.** определять оптимальные способы обеспечения информационной безопасности;  **У7.** проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;  **У8.** проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;  **У9.** разрабатывать политику безопасности сетевых элементов и логических сетей;  **У10.** выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;  **У11.** производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;  **У12.** конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;  **У13.** защищать базы данных при помощи специализированных программных продуктов;  **У14.** защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами. | Практические работы 1,  Практические работы 2,  Практические работы 3,  Практические работы 4,  Практические работы 5,  Практические работы 6,  Наблюдение за процессом выполнения,  Самооценка и оценка практических работ. |
| **должен иметь практический опыт:** |  |
| **ПО 1**. подготовки рабочих мест, оборудования, материалов и инструментов для выполнения штукатурных и декоративных работ в соответствии с инструкциями и регламентами;  **ПО 2.** выполнения подготовительных работ, подготовке оснований и поверхностей под штукатурку, приготовлении штукатурных и декоративных растворов и смесей, выполнении оштукатуривания поверхностей различной степени сложности и их ремонт; | Экспертная оценка выполнения практических работ:  Практические работы 1,  Практические работы 2,  Практические работы 3,  Практические работы 4,  Практические работы 5,  Практические работы 6. |

**ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ**

|  |  |  |  |
| --- | --- | --- | --- |
| **Дата** | **Содержание изменения и дополнения** | **№ страницы, пункт** | **Автор** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |