

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**ХАБАРОВСКИЙ ИНСТИТУТ ИНФОКОММУНИКАЦИЙ
(ФИЛИАЛ)**

**ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ**

ВЫСШЕГО ОБРАЗОВАНИЯ

**«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»**

СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ 02.01

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ**

для специальности

11.02.11 «Сети связи и системы коммутаций»

(базовый уровень)

Хабаровск
2016 г.

Программа учебной практики разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальностям среднего профессионального образования (далее – СПО)

11.02.11 Сети связи и системы коммутации

код

наименование специальности (профессии)

Разработчики:

Вдовина О.П – преподаватель первой категории ХИИК ФГБОУ ВО СибГУТИ
Ф.И.О., ученая степень, звание, должность,

Ф.И.О., ученая степень, звание, должность,

Ф.И.О., ученая степень, звание, должность,

Рецензент:

Клепиков С. И. – профессор, д.т.н, завкафедрой АЭС и ЦТРВ

Рассмотрена на заседании кафедры « АЭС и ЦТРВ»

Протокол № _____ от «20» _____ 20__ г.
Зав. кафедрой _____ / Клепиков С. И./

Утверждена на заседании Методического совета

Протокол № _____ от « » _____ 20__ г.

Утверждена на заседании Методического совета

Протокол № _____ от « » _____ 2016__ г.

Зам. директора по УР _____

/ Капитунова О. А. /
М.П.



Рабочая программа учебной практики УП 02. 01 разработана на основе Федерального государственного образовательного стандарта (далее – ФГОСЗ+) по специальностям среднего профессионального образования (далее – СПО)

11.02.11 Сети связи и системы коммутации

код

наименование специальности (профессии)

Разработчики:

Вдовина О. П. – преподаватель первой категории ХИИК ФГБОУ ВПО СибГУТИ

Рецензенты:

Клепиков С. И. – профессор, д.т.н, завкафедрой АЭС и ЦТРВ

СОГЛАСОВАНО С РАБОТОДАТЕЛЕМ

*Начальник участка
Систем коммутации
Станционного цеха ГЦТЭТ*



Литвинов Р.В.

СОДЕРЖАНИЕ

| | стр. |
|--|------|
| 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ | 5 |
| 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ | 7 |
| 3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ | 8 |
| 4 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ПРАКТИКИ | 15 |
| 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ | 17 |

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи

1.1. Область применения программы

Программа учебной практики – является частью основной профессиональной образовательной программы федерального государственного образовательного стандарта среднего профессионального образования по специальностям СПО 11.02.11 «Сети связи и системы коммутации» для профессиональной образовательной организации (базовой и углубленной подготовки) в части освоения основного вида профессиональной деятельности (ВПД): **Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи** и соответствующих профессиональных компетенций (ПК):

1. Использование программных и аппаратных средства защиты информации в телекоммуникационных системах и сетях связи;
2. Применение системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктур с выдачей рекомендации по их устранению;
3. Обеспечение безопасного администрирования телекоммуникационных систем и информационно-коммуникационных сетей связи.

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

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающихся в области обеспечения безопасности информации путем обучения квалифицированных специалистов по вопросам обеспечения безопасности информации в телекоммуникационных системах и информационно-коммуникационных сетях связи в ходе освоения учебной практики должен:

По профессиональному модулю ПМ.02

уметь:

- выявлять каналы утечки информации;
- определять необходимые средства защиты;
- проводить аттестации объекта защиты (проверки уровня защищенности);
- разрабатывать политику безопасности для объекта защиты;
- устанавливать, настраивать специализированное оборудование по защите информации;
- выявлять возможные атаки на автоматизированные системы;
- устанавливать и настраивать программные средства защиты автоматизированных систем и информационно-коммуникационных сетей;
- проводить конфигурирование автоматизированных систем и информационно-коммуникационных сетей;
- проверять защищенность автоматизированных систем и информационно-коммуникационных сетей;
- проводить защиту баз данных;
- организовать защиту в различных операционных системах и средах;
- шифровать информацию;
- классифицировать угрозы информационной безопасности;
- проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;

- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
 - использовать программные продукты, выявляющие недостатки систем защиты;
 - производить установку и настройку средств защиты;
 - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
 - выполнять тестирование систем с целью определения уровня защищенности;
 - использовать программные продукты для защиты баз данных;
 - применять криптографические методы защиты информации;

знать:

- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей;
- возможные способы несанкционированного доступа;
- нормативно-правовые и законодательные акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- собственные средства защиты различных операционных систем и сред;
- способы и методы шифрования информации

1.3. Количество часов на освоение программы учебной практики: всего – 36 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы учебной практики является овладение обучающимися видом профессиональной деятельности (ВПД) **Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Для базовой и углубленной подготовки:

| Код | Наименование результата обучения |
|---------|--|
| ПК 2.1. | Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи |
| ПК 2.2 | Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению |
| ПК 2.3. | Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи |
| ОК 1 | Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес. |
| ОК 2 | Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. |
| ОК 3 | Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. |
| ОК 4 | Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. |
| ОК 5 | Использовать информационно-коммуникационные технологии в профессиональной деятельности. |
| ОК 6 | Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями. |
| ОК 7 | Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий. |
| ОК 8 | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации. |
| ОК 9 | Ориентироваться в условиях частой смены технологий в профессиональной деятельности. |

3. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

3.1. Тематический план учебной практики

| Код профессиональных компетенций | Наименования разделов производственной практики по профессиональным модулям | Всего часов |
|----------------------------------|---|-------------|
| 1 | 2 | 3 |
| ПК 2.1-.2.3 ОК 4, ОК 5, ОК 8 | УП.2.01 | 36 |
| Всего: | | 36 |

3.2. Тематический план и содержание учебной практики УП.2.01

| Наименование разделов и тем | Содержание учебного материала, лабораторные работы и практические занятия) | Объем часов | Уровень освоения |
|---|---|-------------|------------------|
| 1 | 2 | 3 | 4 |
| УП.2.01 Учебная практика | 4 курс | 36 | |
| Тема 1 Криптографические алгоритмы шифрования. | Изучение основных симметричных и асимметричных криптоалгоритмов шифрования. | 6 | |
| Тема 2 Электронно-цифровая подпись | Создание и проверка цифровой электронной подписи. Практическое применение ViPNet CryptoService | 6 | |
| Тема 3 Программно-аппаратные средства защиты информации | Изучение основных программно-аппаратных средств защиты информации. Построение систем антивирусной защиты телекоммуникационных систем и сетей. | 6 | |
| Тема 4 Программный комплекс ViPNet Administrator | Изучение программного комплекса ViPNet Administrator (Центр управления сетью, Удостоверяющий и ключевой центр) | 6 | |
| Тема 5 Настройка и конфигурирование VPN-туннелей | Настройка и конфигурирование VPN-туннелей. Первичная конфигурация сети ViPNet. | 6 | |
| Тема 6 Межсетевые экраны. Состав программного обеспечения ViPNet OFFICE Firewall. | Изучение программного обеспечения ViPNet OFFICE Firewall. Межсетевые экраны Настройка сетевых фильтров | 6 | |

4. УСЛОВИЯ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие:

Учебных кабинетов, оснащенных персональными компьютерами с выходом в сеть Internet, программами эмуляторов и симуляторов;

Для выполнения лабораторных и практических работ необходимо иметь оборудование:

конфигурации и администрирования сетевых операционных систем, межсетевые экраны, операционные системы WINDOWS, LINUX, UNIX, NOVELL и др., антивирусные программы, криптоалгоритмы, ПО VipNet

Реализация программы учебной практики, происходит сосредоточенно после освоения всего или части междисциплинарного курса.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Учебники

1. Т.Л.Партыка, И.И.Попов Информационная безопасность Москва, ИД «Форум», ИНФРА-М, 2008.
2. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность: Учебное пособие для сред. проф. образования -М. «Академия», 2009.

Дополнительные источники:

Учебники и учебные пособия

1. Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шелупанов Основы информационной безопасности. Москва, Горячая линия – Телеком, 2006
2. В.Ф.Шаньгин Информационная безопасность комплексных систем и сетей. Москва, ИД «Форум», ИНФРА-М, 2008
3. П.Н. Башлы Информационная безопасность. Ростов-на-Дону Феникс.2006
4. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации. Составители А.П.Зайцев, А.А.Шелупанов. Издательство Томского государственного университета систем управления и радиоэлектроники. 2004
5. Защита информации в системах мобильной связи. Учебное пособие. Москва, Горячая линия – Телеком, 2009
6. Технические средства обеспечения информационной безопасности
7. Часть 1. Технические каналы утечки информации
8. Часть 2. Средства защиты информации от утечки по техническим каналам. Учебное пособие, Томск, 2004
9. П.Б.Хорев Методы и средства защиты информации в компьютерных системах Москва, Издательский центр «Академия», 2008
10. А.В.Соколов, О.М.Степанюк Методы информационной защиты объектов и компьютерных сетей – М.: ООО «Фирма «Издательство АСТ» 2000.
11. Ю.В.Романец, П.А.Тимофеев, В.Ф.Шаньгин Защита информации в компьютерных системах и сетях Москва, «Радио и связь», 1999
12. Д.В.Склярков Искусство защиты и взлома информации СПб.: БХВ-Петербург,2004
13. Б.А.Феденко, И.В.Макаров Безопасность сетевых ОС
14. О.М.Раводин, В.О.Раводин Безопасность операционных систем. Томск, Томский государственный университет систем управления и радиоэлектроники. 2005

1. Мир ПК
 2. Первая миля
 3. Электросвязь
 4. Сети
 5. Мир связи
 6. Технологии и средства связи
 7. Радио
 8. Мир ПК+СД
 9. Мобильные компьютеры +СД
 10. Системный администратор
 11. Системы безопасности.
 12. Сети и системы связи
 13. Мобильные телекоммуникации
 14. Технологии и средства связи
 15. Радиоаматер. Практическая радиоэлектроника
 16. Ремонт электронной техники
 17. Мир связи Connect
 18. Мобильные системы
 19. Радиомир
 20. Сети NETWORK WORLD
- 3. Интернет Ресурсы**

www.guardofinform.narod.ru/bibl_3.htm

1. www.minsvyaz.ru Официальный сайт Министерства информационных технологий и связи.
2. www.sotovik.ru Информационный сайт, посвященный телекоммуникациям: обзоры рынка, новости операторов.
3. www.telecomru.ru Экспертный портал "Телекоммуникации России" – независимое сетевое СМИ.
4. www.comnews.ru Новости рынка телекоммуникаций России и СНГ.
5. www.mobail-review.com Сайт, посвященный мобильным устройствам и технологиям, новостям операторов связи, рекламным акциям.
6. www.gptelecom.ru Законы РФ, постановления Правительства, документы Министерства связи и массовых коммуникаций РФ, технические документы и т.д.
7. www.osp.ru , www.pcmag.ru , www.crn.ru , www.elrussia.ru , www.kit-e.ru , www.globus-telecom.com , www.d-link.ru , www.intuit.ru , www.connect.ru , www.qwerty.ru , www.elsv.ru , www.ccc.ru Информационно-справочные системы.

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к учебной практике для получения первичных профессиональных навыков в рамках профессионального модуля является освоение учебной практики для получения первичных профессиональных навыков профессионального модуля ПМ 02 «**Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи**»

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, осуществляющих руководство практикой:

Инженерно-педагогический состав: дипломированные специалисты – преподаватели междисциплинарных курсов, имеющие высшее образование по профилю модуля и специальности подготовки.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Для базовой и углубленной подготовки:

| Результаты (освоенные профессиональные компетенции) | Основные показатели оценки результата | Формы и методы контроля и оценки |
|--|--|---|
| Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи | <ul style="list-style-type: none"> – Четкое понимание проблем информационной безопасности в сфере телекоммуникаций; – Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления; – Выбор механизмов и средств обеспечения информационной безопасности - программных и программно-аппаратных; – Грамотно оформлять документацию для лицензирования работ в области информационной безопасности; – Разрабатывать политики в области информационной безопасности; | Текущий контроль в форме: - защиты лабораторных работ; - исследовательско-поисковый характер работы по тематике модуля с использованием Internet. |
| Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению | <ul style="list-style-type: none"> – Расчет рисков в области информационной безопасности и выдача рекомендаций по их устранению; – Владеть сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и информационно-коммуникационных сетях связи; – Владеть технологией аутентификации; – Обеспечивать технологию защиты межсетевого обмена данными; – Построение системы антивирусной защиты телекоммуникационных систем и информационно-коммуникационных сетей. | |
| Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи | <ul style="list-style-type: none"> – Выбор и использование пакетов прикладных программ для безопасного администрирования сетевых операционных систем; – Обеспечение программными и программно-аппаратными методами безопасности сетей доступа, объединенных сетей и управления телекоммуникационными сетями. | |

Формы и методы контроля и оценки результатов обучения должны позволить проверку у обучающихся не только сформированности профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Для базовой и углубленной подготовки:

| Результаты (освоенные общие компетенции) | Основные показатели оценки результата | Формы и методы контроля и оценки |
|--|---|---|
| Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес | - своевременное и качественное применение компетенций, умений и знаний предусмотренных Основной Профессиональной Образовательной Программой по специальности. | Текущий контроль в форме: - защиты лабораторных работ;; - электронное тестирование. |
| Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество | – выбор и применение методов и способов решения профессиональных задач в области обеспечения безопасности телекоммуникационных систем и информационно-коммуникационных сетей; – оценка эффективности и качества выполнения; | Зачеты по учебной практике. |
| Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях. | решение стандартных и нестандартных профессиональных задач по обеспечению безопасности телекоммуникационных систем и информационно-коммуникационных сетей; Оперативно принимать решение стандартных и нестандартных профессиональных задач и организовать деятельность по обеспечению безопасности систем. | |
| Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития. | – эффективный поиск необходимой информации; – использование различных источников, включая электронные базы данных. -анализ полученной информации и применение ее для решения профессиональных задач. | |
| Использовать информационно-коммуникационные технологии (для | – работа с различными операционными системами и средами, программно-аппаратными и программными | |

| | | |
|---|--|--|
| <p>совершенствования*) в профессиональной деятельности</p> | <p>– внедрение современных технологий*;</p> | |
| <p>Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.</p> <p>Работать в коллективе и команде, обеспечивать ее сплочение эффективно общаться с коллегами, руководством, потребителями.</p> | <p>– взаимодействие с обучающимися и преподавателями в ходе обучения, а также с членами коллектива предприятия во время производственной практики;</p> <p>-руководство группой, бригадой и эффективная организация деятельности для выполнения работ*;</p> | |
| <p>Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.</p> <p>Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий*.</p> | <p>– самоанализ и коррекция результатов собственной работы, оценка деятельности по конечному результату.</p> <p>-организация деятельности членов команды;</p> <p>- анализ результатов и оценка деятельности подчиненных и собственной работы.</p> | |
| <p>Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации</p> | <p>– организация самостоятельных занятий при изучении профессионального модуля;</p> <p>– -планирование повышения квалификации.</p> | |
| <p>Ориентироваться в условиях частой смены технологий в профессиональной деятельности.</p> <p>Быть готовым к смене технологий в профессиональной деятельности*.</p> | <p>– анализ инноваций в области программного обеспечения, развития отрасли,</p> <p>– расширение кругозора в профессиональной деятельности.</p> <p>-освоение новых технологий*;</p> | |
| <p>Исполнять воинскую обязанность, в том</p> | <p>– с честью выполнять гражданский долг в любой сфере деятельности и</p> | |

| | | |
|--|---|--|
| числе с применением полученных профессиональных знаний (для юношей). | применять полученные профессиональные компетенции | |
|--|---|--|

Рабочая программа Учебной практики ПМ 02 «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммутационных сетей связи» разработана на основе Федеральной государственной образовательной стандарта по специальности среднего профессионального образования 11.02.11 «Сети связи и системы коммутации»

Разработчик: _____

Вдовина О.П. – преподаватель первой категории ХИИК (филиал) ФГБОУ ВО «СибГУТИ»
