**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

ХАБАРОВСКИЙ ИНСТИТУТ ИНФОКОММУНИКАЦИЙ
(ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
(ХИИК СибГУТИ)

СРЕДНЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

# РАБОЧАЯ ПРОГРАММА

# УП.03.01 УЧЕБНАЯ ПРАКТИКА

для специальности
11.02.10 «Радиосвязь, радиовещание и телевидение»

(базовый уровень)

Хабаровск
2016 г.

Рабочая программа учебной практики УП.03.01 разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 11.02.10 Радиосвязь, радиовещание и телевидение

Разработчики:

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

Воронина Ю.В. – преподаватель ХИИК СибГУТИ
Ф.И.О., ученая степень, звание, должность.

Рецензент:

Ананьин А.В. доцент, к.т.н. ХИИК СибГУТИ

Рассмотрена на заседании кафедры«Автоматической электросвязи и цифрового телерадиовещания»

Протокол № 9 от « 07 » июня 2016 г.
Зав. кафедрой _____ / С.И.Клепиков/

Утверждена на заседании Методического совета
Протокол № 10 от « 08 » июня 2016г.

Зам.директора по УНР _____ /О.А.Капитунова/

Согласовано с работодателем _____ / Пинегин П.А. /

**СОДЕРЖАНИЕ**

## 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

### 1.1. Область применения программы

Программа учебной практики УП.03.01 – является частью основной профессиональной образовательной программы федерального государственного образовательного стандарта среднего профессионального образования по специальности СПО **11.02.10 Радиосвязь, радиовещание и телевидение»** для профессиональной образовательной организации в части освоения основного вида профессиональной деятельности (ВПД): **Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания** и соответствующих профессиональных компетенций (ПК):

ПК 3.1 Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания

ПК 3.2 Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.;

ПК 3.3 Обеспечивать безопасное администрирование сетей вещания.

### 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-коммутационных сетях связи в ходе освоения учебной практики **должен**:

**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;

- законодательные и нормативные правовые акты в области информационной безопасности;

- правила проведения возможных проверок;

- этапы определения конфиденциальности документов объекта защиты;

- структуру систем условного доступа и принцип их работы;

- 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 УЧЕБНОЙ ПРАКТИКИ

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:

| Код | Наименование результата обучения |
|---|---|
| ПК 3.1. | Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания. |
| ПК 3.2 | Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению. |
| ПК 3.3 | Обеспечивать безопасное администрирование сетей вещания. |
| 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 учебной практики по профессиональным модулям | Всего часов |
|---|---|---|
| 1 | 2 | 3 |
| ПК 3.1 - 3.3 | УП.03.01 | 36 |
| | Всего: | 36 |

### 3.2. Тематический план и содержание учебной практики УП.03.01

| Наименование разделов и тем | Содержание учебного материала, лабораторные работы и практические занятия) | Объем часов | Уровень освоения |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **УП.03.01 Учебная практика** | **4 курс** | **36** | |
| **Тема 1** Криптографические алгоритмы шифрования. | Изучение основных симметричных и ассиметричных криптоалгоритмов шифрования. | **6** | **3** |
| **Тема 2** Электронно-цифровая подпись | Создание и проверка цифровой электронной подписи. Практическое применение ViPNet CryptoService | **6** | **3** |
| **Тема 3** Программно-аппаратные средства защиты информации | Изучение основных программно-аппаратных средств защиты информации. Построение систем антивирусной защиты телекоммуникационных систем и сетей. | **6** | **3** |
| **Тема 4** Программный комплекс ViPNet Administrator | Изучение программного комплекса ViPNet Administrator (Центр управления сетью, Удостоверяющий и ключевой центр) | **6** | **3** |
| **Тема 5** Настройка и конфигурирование VPN-туннелей | Настройка и конфигурирование VPN-туннелей. Первичная конфигурация сети ViPNet. | **6** | **3** |
| **Тема 6** Межсетевые экраны. Состав программного обеспечения ViPNet OFFICE Firewall. | Изучение программного обеспечения ViPNet OFFICE Firewall. Межсетевые экраны Настройка сетевых фильтров | **6** | **3** |

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

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

Реализация программы учебной практики 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

1. Учебники:

1. Шаньгин В.Ф.Комплексная защита информации в корпоративных сетях: учеб. пособ. – М.: Форум-Инфра-М,2013

2. Величко В.В. Модели и методы повышения живучести современных систем связи [Электронный ресурс]/ Величко В.В., Попков Г.В., Попков В.К.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2014.— 270 с.— Режим доступа: http://www.iprbookshop.ru/37126.— ЭБС «IPRbooks», по паролю

3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks», по паролю

4. Аверченков А.В. и др. Разработка системы технической защиты информации - Брянск.: БГТУ,2012/ эл. ресурс ЭБС iprbooks.

5. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.— Режим доступа: http://www.iprbookshop.ru/29257.— ЭБС «IPRbooks», по паролю

6. Аверченков В.И. Организационная защита информации [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И., Рытов М.Ю.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 184 с.— Режим доступа: http://www.iprbookshop.ru/7002.— ЭБС «IPRbooks», по паролю

7. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов/ Аверченков В.И.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 268 с.— Режим доступа: http://www.iprbookshop.ru/6991.— ЭБС «IPRbooks», по паролю

8. Аверченков В.И. Защита персональных данных в организации [Электронный ресурс]: монография/ Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 124 с.— Режим доступа: http://www.iprbookshop.ru/6993.— ЭБС «IPRbooks», по паролю

9. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 с.— Режим доступа: http://www.iprbookshop.ru/7000.— ЭБС «IPRbooks», по паролю

10. Аверченков В.И. Мониторинг и системный анализ информации в сети Интернет [Электронный ресурс]: монография/ Аверченков В.И., Рощин С.М.— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 160 с.— Режим доступа: http://www.iprbookshop.ru/7001.— ЭБС «IPRbooks», по паролю

2. Нормативно-правовые источники

1. Конституция Российской Федерации (от 12.12.1993 г.).
2. Федеральный закон Российской Федерации «Об информации, информатизации и защите информации» (№ 24-03 от 20.02.1995 г.).
3. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).
4. Федеральный закон Российской Федерации «О государственной тайне» (№ 5485-1 от 06.10.1997 г.).
5. Указ Президента РФ «Перечень сведений конфиденциального характера» (№ 188 06.03.1997 г.).
6. Федеральный закон Российской Федерации «О персональных данных» (№ 152 от 27.07.2006 г.).
7. Федеральный закон Российской Федерации «Об электронной цифровой подписи» (№ 1-ФЗ от 26.12.2001 г.).

3. Интернет-источники:

1. www.minsvyaz.ru Официальный сайт Министерства информационных технологий и связи.
2. http://habrahabr.ru/ Социальное СМИ об IT
3. www.wikipedia.org Свободная энциклопедия
4. http://www.scrf.gov.ru/ Официальный сайт Совета безопасности Российской Федерации

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

Обязательным условием допуска к учебной практике УП.03.01 для получения первичных профессиональных навыков в рамках профессионального модуля ПМ.03 «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ВЕЩАНИЯ», является освоение программы соответствующих междисциплинарных курсов МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания и МДК.03.02 Технология использования систем условного доступа в сетях вещания.

**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

| Результаты (освоенные профессиональные компетенции) | Основные показатели оценки результата | Формы и методы контроля и оценки |
|---|---|---|
| ПК 3.1 Использовать программно-аппаратные средства защиты информации в системах радиосвязи и сетях вещания | – Четкое понимание проблем информационной безопасности в сфере телекоммуникаций;<br>– Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления;<br>– Выбор механизмов и средств обеспечения информационной безопасности - программных и программно-аппаратных;<br>– Грамотно оформлять документацию для лицензирования работ в области информационной безопасности;<br>– Разрабатывать политики в области информационной безопасности; | Текущий контроль в форме:<br>- защиты лабораторных работ;<br>- исследовательско - поисковый характер работы по тематике модуля с использованием Internet. |
| ПК 3.2 Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению | – Расчет рисков в области информационной безопасности и выдача рекомендаций по их устранению;<br>– Владеть сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и информационно-коммуникационных сетях связи;<br>– Владеть технологией аутентификации;<br>– Обеспечивать технологию защиты межсетевого обмена данными;<br>– Построение системы антивирусной защиты телекоммуникационных систем и информационно-коммуникационных сетей. | |
| ПК 3.3 Обеспечивать безопасное администрирование сетей вещания | – Выбор и использование пакетов прикладных программ для безопасного администрирования сетевых операционных систем;<br>– Обеспечение программными и программно-аппаратными методами безопасности сетей доступа, объединенных сетей и управления телекоммуникационными сетями. | |

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

| **Результаты (освоенные общие компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ОК 1. 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:<br>- защиты лабораторных работ;;<br>- электронное тестирование.<br><br>Зачет по учебной практике. |
| ОК 2. 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;<br>– оценка эффективности и качества выполнения; | |
| ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. | решение стандартных и нестандартных профессиональных задач по обеспечению безопасности телекоммуникационных систем и информационно-коммуникационных сетей; | |
| ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. | – эффективный поиск необходимой информации;<br>– использование различных источников, включая электронные базы данных. | |
| ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности | – работа с различными операционными системами и средами, программно-аппаратными и программными средствами<br>– внедрение современных технологий; | |
| ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями. | – взаимодействие с обучающимися и преподавателями в ходе обучения, а также с членами коллектива предприятия во время производственной практики;<br>-руководство группой, бригадой и эффективная организация деятельности для выполнения работ; | |

| | | |
|---|---|---|
| ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий. | – самоанализ и коррекция результатов собственной работы, оценка деятельности по конечному результату.<br>-организация деятельности членов команды. | |
| ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации | – организация самостоятельных занятий при изучении профессионального модуля;<br>– планирование повышения квалификации. | |
| ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности. | – анализ инноваций в области программного обеспечения, развития отрасли;<br>– расширение кругозора в профессиональной деятельности;<br>- освоение новых технологий. | |

## 1. Пояснительная записка

Комплект оценочных средств УП 03.01Учебная практика разработан на основе:
1) Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее – СПО), утвержденного приказом Министерства образования и науки Российской Федерации № 812от 28 июля 2014 г. 11.02.10 Радиосвязь, радиовещание и телевидение.

### Объем учебной дисциплины и виды учебной работы

**(очная форма обучения)**

| **Вид учебной работы** | **Количество часов** |
|---|---|
| **Максимальная учебная нагрузка (всего)** | 36 |
| **Обязательная аудиторная учебная нагрузка (всего)** | 36 |
| в том числе: | |
| практические занятия | |
| лабораторные занятия | 36 |
| **Консультации** | |
| **Самостоятельная работа обучающегося (всего)** | |
| ***Итоговая аттестация*** *в форме дифференцированного зачета* | |

**(заочная форма обучения)**

| **Вид учебной работы** | **Количество часов** |
|---|---|
| **Максимальная учебная нагрузка (всего)** | 36 |
| **Обязательная аудиторная учебная нагрузка (всего)** | |
| в том числе: | |
| обзорные, установочные занятия | |
| практические занятия | |
| **Консультации** | |
| **Самостоятельная работа обучающегося (всего)** | |
| ***Итоговая аттестация*** *в форме дифференцированного зачета* | |

Учебная практика УП 03.01 входит в профессиональный модуль ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания.

Техник должен обладать **общими компетенциями,** включающими в себя способность:

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 личного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), 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.

**Профессиональными компетенциями,** включающими в себя способность:

ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.

ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование сетей вещания.

**2. Сведения об иных дисциплинах (преподаваемых в том числе на других кафедрах) участвующих в формировании данных компетенций:**

| Наименование дисциплины, профессионального модуля, участвующие в формировании компетенций | Компетенции |
|---|---|
| ЕН.01 Математика | ОК 1-9 |
| ЕН.02 Компьютерное моделирование | ОК 1-9, ПК3.1-3.3 |
| ОП.01 Теория электрических цепей | ОК 1-9 |
| ОП.02 Электронная техника | ОК 1-9 |
| ОП.03 Теория электросвязи | ОК 1-9 |
| ОП.04 Вычислительная техника | ОК 1-9 |
| ОП.05 Электрорадиоизмерения | ОК 1-9 |
| ОП.06 Основы телекоммуникаций | ОК 1-9 |
| ОП.08 Охрана труда | ОК 1-9, ПК3.1-3.3 |
| ОП.09 Компьютерная графика | ОК 1-9 |
| ОП.10 Технические средства информатизации | ОК 1-9 |
| ОП.11 Сети радиосвязи | ОК 1-9 |
| ОП.12 Правовое обеспечение профессиональной деятельности | ОК 1-9 |
| ОП.13 Информационные технологии | ОК 1-9, ПК 3.1 |
| ОП.14 Безопасность жизнедеятельности | ОК 1-9, ПК 3.1-3.3 |
| МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания | ОК 1-9 |
| МДК.03.02 Технология использования систем условного доступа в сетях вещания | ОК 1-9 |

Основными формами проведения текущего контроля знаний на занятиях являются устный опрос, выполнение и защита лабораторных работ.

**Паспорт**

**фонда оценочных средств по УП.03.01 Учебная практика**

| № п/п | Контролируемые разделы | Код контролируемой компетенции (или ее части) | Наименование оценочного средства |
|---|---|---|---|
| 1 | **Тема 1** Криптографические алгоритмы шифрования. | ОК 1-9 ПК 1.1 – 1.5 | лабораторная работа 1 |
| 2 | **Тема 2** Электронно-цифровая подпись | ОК 1-9 ПК1.1-ПК 1.5 | лабораторная работа 2 |
| 3 | **Тема 3** Программно-аппаратные средства защиты информации | ОК 1-9 ПК1.1-ПК 1.5 | лабораторная работа 3 |
| 4 | **Тема 4** Программный комплекс ViPNet Administrator | ОК 1-9 ПК 1.3 | лабораторная работа 4 |
| 5 | **Тема 5** Настройка и конфигурирование VPN-туннелей | ОК 1-9 ПК1.1-ПК 1.5 | лабораторная работа 5 |
| 6 | **Тема 6** Межсетевые экраны. Состав программного обеспечения ViPNet OFFICE Firewall. | ОК 1-9 ПК 1.3 | лабораторная работа 6 |

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Хабаровский институт инфокоммуникаций (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(ХИИК СибГУТИ)

Кафедра Автоматической электросвязи и цифрового телерадиовещания

**Перечень вопросов текущего контроля**

**по УП.03.01 Учебная практика**

1. Понятие информационной безопасности
2. Характеристика составляющих информационной безопасности
3. Место информационной безопасности в системе национальной безопасности
4. Концептуальная модель защиты информации
5. Классификация и анализ угроз информационной безопасности в телекоммуникационных системах
6. Виды уязвимости информации и формы ее проявления.
7. Понятие конфидициальной информации. Грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне
8. Уровни информационной безопасности
9. Нормативно-правовые основы информационной безопасности
10. Составление комплекта документации для лицензирования работ и услуг в области защиты информации (ФСТЭК)
11. Лицензирование и сертификация в области защиты информации. Стандартизация информационной безопасности
12. Криптографическая защита
13. Симметричные криптоалгоритмы
14. Ассиметричные криптоалгоритмы
15. Поточные шифры
16. Блочные шифры
17. Гаммирование
18. Сеть Фейстеля
19. Алгоритм DES
20. Создание и проверка цифровой электронной подписи
21. Вредоносное ПО и защита от него
22. Антивирусное ПО
23. Проблемы безопасности протоколов TCP/IP. Сканирование сети
24. ARP атаки
25. Туннелирование
26. Экранирование и межсетевые экраны
27. Классификация межсетевых экранов
28. Пакетная фильтрация
29. Алгоритм RSA
30. Вопросы безопасности применения межсетевых экранов.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
Хабаровский институт инфокоммуникаций (филиал)
Федерального государственного бюджетного образовательного учреждения
высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(ХИИК СтбГУТИ)

Кафедра Автоматическая электросвязь и цифровое телерадиовещание

УТВЕРЖДЕН
на заседании кафедры АЭС и ЦТРВ
«1» июня 2016 г. протокол№ 9
Заведующий кафедрой
_____Клепиков С. И.

# КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ

К дифференцированному зачету по УП 03.01 Учебная практика

11.02.10 Радиосвязь, радиовещание и телевидение

Техник

Квалификация (степень) выпускника

Хабаровск
2016 г.

| Зав. кафедрой АЭС и ЦТРВ<br>_____Клепиков С. И. | Билет №20<br>Учебная практика УП 03.01 |
|---|---|

ФИО студента_____

Теоретический блок

1) Симметричные алгоритмы.
2) Проблемы безопасности протоколов TCP/IP
3) Гаммирование

Практический блок

Известно, что при использовании шифра пропорциональной замены каждой русской букве поставлено в соответствие одно или несколько трехзначных чисел по таблице замен:

| | |
|---|---|
| А 760128350201 | С 800767105 |
| Б 101 | Т 759135214 |
| В 210106 | У 544 |
| Г 351 | Ф 560 |
| Д 129 | Х 768 |
| Е 761130802352 | Ц 545 |
| Ж 102 | Ч 215 |
| З 753 | Ш 103 |
| И 762211131 | Щ 752 |
| К 754764 | Ъ 561 |
| Л 132354 | Ы 136 |
| М 755742 | Ь 562 |
| Н 763756212 | Э 750 |
| О 757213765133353 | Ю 570 |
| П 743766 | Я 216104 |
| Р 134532 | Пробел 751769758801849035 |

| | |
|---|---|
| Зав. кафедрой АЭС и ЦТРВ<br>_____Клепиков С. И. | Экзаменационный билет №19<br>Учебная практика УП 03.01 |

ФИО студента_____

Теоретический блок

1) Создание и проверка электронной подписи.
2) Вопросы безопасности применения межсетевых экранов
3) Антивирусное программное обеспечение.

Практический блок

Определить время (t) перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10. Длина пароля (k)-6. Принять скорость перебора (s)-10 паролей в секунду, после каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд.

| | |
|---|---|
| Зав. кафедрой АЭС и ЦТРВ<br>_____Клепиков С. И. | Экзаменационный билет №18<br>Учебная практика УП 03.01 |

ФИО студента_____

Теоретический блок

1) Поточные шифры
2) Классификация межсетевых экранов
3) Алгоритм DES.

Практический блок

Расшифруйте сообщения, зашифрованное методом перестановки с фиксированным периодом d=8 с ключом 64275813:

СЛПИЬНАЕ

РОИАГДВН

| | |
|---|---|
| Зав. кафедрой АЭС и ЦТРВ<br>_____Клепиков С. И. | Экзаменационный билет №16<br>Учебная практика УП 03.01 |

ФИО студента_____

Теоретический блок

1) ARP-атаки.
2) Туннелирование.
3) Симметричные криптоалгоритмы.

Практический блок

Зашифровать с помощью шифра Вижинера и ключа ЯБЛОКО сообщения:

КРИПТОСТОЙКОСТЬ

ГАММИРОВАНИЕ

| | |
|---|---|
| Зав. кафедрой АЭС и ЦТРВ<br>_____Клепиков С. И. | Экзаменационный билет №15<br>Учебная практика УП 03.01 |

ФИО студента_____

Теоретический блок

1) Уровни информационной безопасности.
2) Вредоносное программное обеспечение и защита от него.
3) Вопросы безопасности применения межсетевых экранов.

Практический блок

Первый байт фрагмента текста, зашифрованного методом гаммирования (по модулю 2) в шестнадцатеричном виде имеет вид А6. На него накладывается по модулю два 4-х битовая гамма 1011. Что получится после шифрования?

| | |
|---|---|
| Зав. кафедрой АЭС и ЦТРВ<br>_____Клепиков С. И. | Экзаменационный билет №14<br>Учебная практика УП 03.01 |

ФИО студента_____

Теоретический блок

1) Туннелирование.
2) Канальное шифрование.
3) Виды уязвимости информации и формы ее проявления

Практический блок

Первый байт фрагмента текста в шестнадцатеричном виде имеет вид А5. На него накладывается по модулю два 4-х битовая гамма 0111. Что получится после шифрования?

Критерии оценки:

- оценка «отлично» выставляется обучающемуся, если обучающийся ответил на три вопроса, теоретической и практической части, построил схемы, полностью раскрыл содержание вопроса.

- оценка «хорошо» - обучающийся ответил на два вопроса, теоретической и два вопроса практической части, построил схемы, полностью раскрыл содержание вопроса.

- оценка «удовлетворительно» - обучающийся ответил на два-один вопроса, теоретической и один два вопроса практической части не полностью, построил схемы, не полностью раскрыл содержание вопроса.

- оценка «неудовлетворительно» - обучающийсяне ответил на вопросы или раскрыл два вопроса частично