ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Бурятский институт инфокоммуникаций (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Улан-Удэ

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 03 «ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ»

Специальность: 11.02.09 «Многоканальные телекоммуникационные системы»

Форма обучения: очная

Улан-Удэ
2017

Рассмотрена и одобрена на заседании кафедры
зав. кафедрой телекоммуникационных систем:

_____/А.С.Нестеров /

«01» сентября 2017 г.

УТВЕРЖДАЮ

Заместитель директора по УНР

_____/Т.Г. Батурина/

«04» сентября 2017 г.

Программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее - ФГОС) по специальности (специальностям) среднего профессионального образования (далее СПО) 11.02.09 «Многоканальные телекоммуникационные системы»

Организация разработчик: БИИК ФГБОУ ВО СибГУТИ

Разработчик:
Нестеров Андрей Сергеевич – преподаватель кафедры «Телекоммуникационных систем» БИИК ФГБОУ ВО СибГУТИ.

Эксперты:
Трофимов Дмитрий Васильевич – ведущий специалист отдела обеспечения защиты государственной тайны БФ ПАО Ростелеком.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 «ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ»

1.1. Область применения программы

Программа профессионального модуля (далее - программа) – является частью программы подготовки специалистов среднего звена всоответствии с ФГОС по специальности СПО **11.02.09 Многоканальные телекоммуникационные системы**(базовой подготовки) в части освоения основного вида профессиональной деятельности (ВПД): **Обеспечения информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи**и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Использовать программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.

ПК 3.2. Применять системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке в области телекоммуникаций при наличии среднего (полного) общего образования, опыт работы не требуется.

Программа профессионального модуля может быть использована при повышении квалификации и переподготовке работников связи при наличии профессионального образования.

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

С целью овладения указанным видом профессиональной деятельности исоответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- выявления каналов утечки информации;
- определения необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности);
- разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы;
- установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;

- конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
- проверки защищенности автоматизированных систем и информационно-коммуникационных сетей;
- защиты баз данных;
- организации защиты в различных операционных системах и средах;
- шифрования информации;

уметь:

- классифицировать угрозы информационной безопасности;
- проводить выбор средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- 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;
- нормативные 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;
- средства защиты различных операционных систем и сред;
- способы и методы шифрования информации.

1.3. Количество часов на освоение программы профессионального модуля:

всего **– 180** часов, в том числе:

максимальной учебной нагрузки обучающегося – **144** часа, включая:

- обязательной аудиторной учебной нагрузки обучающегося – **96** часов;

- самостоятельной работы обучающегося – **48** часов;

учебной практики – **36** часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Обеспечения информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи
ПК 3.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению
ПК 3.3	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 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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план

Код профессиональных компетенций	Наименования разделов профессионального модуля*	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)					Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Учебная, часов	Производственная (по профилю специальности),** часов
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Всего, часов	в т.ч., курсовая работа (проект), часов		
1	2	3	4	5	6	7	8	9	10
ПК 3.1 – ПК 3.3	**Раздел 1.** Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**54**	**36**	18		18			
ПК 3.1 – ПК 3.3	**Раздел 2.**Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**126**	**60**	30		30		**36**	
	Производственная практика (по профилю специальности), часов								
	Всего:	**180**	**96**	48		**48**		**36**	

3.2.Содержание обучения по профессиональному модулю ПМ 03

Наименование разделов МДК и тем		Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающихся, курсовой проект (работа)	Объем часов	Уровень освоения
1		2	3	4
Раздел 1. Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи			**54**	
МДК 03.01 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи			**54**	
Тема 1.1. Информационная безопасность.	1	**Основы информационной безопасности** • Понятие информационной безопасности, характеристика ее составляющих. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации. • Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. Виды уязвимости информации и формы ее проявления.	2	2
		• Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации. Модель нарушителя. Модели защиты информационных систем.	2	2
	2	**Правовое обеспечение информационной безопасности.** • Информация как объект права. Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. • Понятие и виды защищаемой информации по законодательству РФ. Система защиты государственной тайны, правовой режим защиты государственной тайны	2	3
	3	**Организационное обеспечение информационной безопасности.**	2	3
	4	• Сущность и сферы действия организационной защиты информации. • Механизмы обеспечения информационной безопасности. Разработка политики безопасности. • Проведение анализа угроз и расчета рисков в области информационной безопасности. Выбор механизмов и средств обеспечения информационной безопасности. Организация работы персонала с конфиденциальной информацией. Разработка инструкций по работе со средствами защиты.		

	5	• Сущность и сферы действия организационной защиты информации. • Механизмы обеспечения информационной безопасности. Разработка политики безопасности. • Проведение анализа угроз и расчета рисков в области информационной безопасности. Выбор механизмов и средств обеспечения информационной безопасности. Организация работы персонала с конфиденциальной информацией. Разработка инструкций по работе со средствами защиты.	2	2
	6	**Администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.** • Технологии защиты данных. • Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, классические алгоритмы шифрования, электронная цифровая подпись, стеганография). Различные технологии аутентификации.	2	3
		• Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы. Построение систем антивирусной защиты телекоммуникационных систем и сетей.	2	2
		• Технологии защиты межсетевого обмена данных. • Технология обеспечения безопасности сетевых операционных систем. Основы технологии виртуальных защищенных сетей VPN. • Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак).	2	2
		• Требования по защите от несанкционированного доступа. Технические средства обеспечения безопасности подвижных объектов.	2	2
		Лабораторные работы	**18**	
	1	Профилактика компьютера от троянских программ	4	
	2	Настройка параметров аутентификации Windows	2	
	3	Классификация способов сетевой адресации.	4	
	4	Расчёт подсетей и хостов, вычисление масок подсети	4	
	5	Настройка фильтрации на маршрутизаторе.	4	
Самостоятельная работа при изучении Раздела ПМ Систематическая проработка электронных конспектов занятий, учебной и специальной технической литературы. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление отчетов к лабораторным и практическим работам и подготовка к их защите.			**18**	
Раздел 2. Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи			**90**	

МДК 03.02 Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи		**90**	
Тема 2.1. Комплексная система защиты информации.	**Сущность и задачи комплексной защиты информации** • Цели, задачи и принципы построения КСЗИ. • Разумная достаточность и экономическая эффективность. • Цели и задачи защиты информации в автоматизированных системах.	2	2
	Принципы организации и этапы разработки КСЗИ. • Разработка политики безопасности и регламента безопасности предприятия. Этапы разработки КСЗИ	2	3
	Факторы, влияющие на организацию КСЗИ. • Характер основной деятельности предприятия. • Состав, объекты и степень конфиденциальности защищаемой информации • Конструктивные особенности предприятия	2	3
	Определение и нормативное закрепление состава защищаемой информации. • Классификация информации по видам тайны и степеням конфиденциальности. • Нормативно-правовые аспекты определения состава защищаемой информации.	2	2
	Определение объектов защиты • Значение носителей защищаемой информации как объектов защиты • Факторы, определяющие необходимость защиты периметра и здания предприятия • Особенности помещений как объектов защиты для работы по защите информации • Состав средств обеспечения, подлежащих защите	2	2
	Дестабилизирующие воздействия на информацию и их нейтрализация • Факторы, создающие угрозу информационной безопасности • Угрозы безопасности информации • Модели нарушителей безопасности АС • Обеспечение безопасности информации в непредвиденных ситуациях • Резервирование информации и отказоустойчивость	2	3
	Определение потенциальных каналов и методов несанкционированного доступа к информации • Технические каналы утечки информации, их классификация • Особенности защиты речевой информации	2	2

	Определение возможностей несанкционированного доступа к защищаемой информации • Методы и способы защиты информации • Механизмы обеспечения безопасности информации • Методика выявления нарушителей, тактики их действий и состава интересующей их информации	2	3
	Определение компонентов КСЗИ • Особенности синтеза СЗИ АС от НСД • Методика синтеза СЗИ • Оптимальное построение системы защиты для АС • Выбор структуры СЗИ АС • Проектирование системы защиты информации для существующей АС	2	3
	Определение условий функционирования КСЗИ • Содержание концепции построения КСЗИ • Объекты защиты • Основные угрозы безопасности информации АС организации • Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов	2	3
	Разработка модели КСЗИ • Общая характеристика задач моделирования КСЗИ • Формальные модели безопасности и их анализ • Формальное построение модели защиты	2	3
	Технологическое и организационное построение КСЗИ • Общее содержание работ по организации КСЗИ • Характеристика основных стадий создания КСЗИ • Назначение и структура технического задания • Предпроектное обследование, технический проект, рабочий проект. Апробация и ввод в эксплуатацию	2	3
	Кадровое обеспечение функционирования комплексной системы защиты информации • Специфика персонала предприятия как объекта защиты • Распределение функций по защите информации • Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа	2	3

	Материально-техническое и нормативно-методическое обеспечение комплексной системы защиты информации • Состав и значение материально-технического обеспечения функционирования КСЗИ • Перечень вопросов ЗИ, требующих документационного закрепления		2	3
	Методы и модели оценки эффективности КСЗИ • Показатель уровня защищенности, основанный на экспертных оценках • Методы проведения экспертного опроса • Экономический подход к оценке эффективности КСЗИ		2	3
	Лабораторные работы		**30**	
	1	Настройка маршрутизатора	4	
	2	Обновление прошивки, настройка пакетов	2	
	3	Настройка подключения по SSH	4	
	4	Отключение неиспользуемых сервисов	2	
	5	Настройка SNMP	2	
	6	Проброс портов	2	
	7	Анализ трафика	2	
	8	Маркировка пакетов	2	
	9	Простые очереди	2	
	10	Дерево очередей	2	
	11	Анализ структуры сети	2	
	12	Настройка пользователей, настройка безопасности	4	

Самостоятельная работа при изучении раздела ПМ Систематическая проработка электронных конспектов занятий, учебной и специальной технической литературы. Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление отчетов к лабораторным и практическим работам и подготовка к их защите.	**30**	
Учебная практика Настройка роутера, Watchdog, Filter, filter с использованием Addresslists, Layer7 filter. Расширенная настройка фильтрации пакетов, VPN (PPTP), VPN (L2TP). маркировки соединения, настройка резервного канала.	**36**	
Всего	**180**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля предполагает наличие лаборатории информационной безопасности и компьютерных мастерских.

Оборудование мастерской и учебных мест мастерской:

- маршрутизатор MikroTikOmniTIK U-5HnD
- компьютеры (10 шт.) и оргтехника;
- программное обеспечение профессионального назначения к выполнению лабораторных работ;
- учебно-методическое обеспечение.

Оборудование лаборатории и рабочих мест лаборатории:

- Локальная вычислительная сеть на 6 компьютеров
- Сетевое оборудование (коммутаторы DLink)
- Мультимедиа оборудование (Web камеры, микрофоны, наушники)

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы:

Основные источники:

1. Голиков А.М. Основы проектирования защищенных телекоммуникационных систем [Электронный ресурс] : учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А.М. Голиков. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. — 396 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/72158.html
2. Долозов Н.Л. Компьютерные сети [Электронный ресурс]: учебно-методическое пособие/ Долозов Н.Л.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2013.— 112 c.— Режим доступа: http://www.iprbookshop.ru/45377.— ЭБС «IPRbooks», по паролю

Дополнительная литература

1. Построение коммутируемых компьютерных сетей [Электронный ресурс]/ Е.В. Смирнова [и др.].— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 428 c.— Режим доступа: http://www.iprbookshop.ru/16723.— ЭБС «IPRbooks», по паролю
2. Практикум по выполнению лабораторных работ по дисциплине Криптографические методы защиты информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2015. — 67 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61738.html
3. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/63099.html

Интернет-ресурсы

доступ к информационным, справочным и поисковым системам
http://www.mikrotik.com/ Сайт компании «Mikrotik».
http://wiki.mikrotik.com/wiki/Main_PageMikrotik Wiki
http://habrahabr.ru/ Социальное СМИ об IT

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ 03

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Использование программно-аппаратные средства защиты информации в многоканальных телекоммуникационных системах, информационно-коммуникационных сетях связи.	• Уметь проводить выборку средств защиты в соответствии с выявленными угрозами;	Текущий контроль в форме: -защиты лабораторных занятий; - наблюдения преподавателя за выполнением конкретного задания; - зачеты по учебной практике и по каждому из МДК; -квалификационный экзамен по профессиональному модулю
ПК 3.2. Применение системы анализа защищенности с целью обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	• Уметь использовать программные продукты для защиты баз данных; • Уметь применять криптографические методы защиты информации; • Уметь использовать программные продукты для защиты баз данных • Иметь опыт установки, настройки специализированного оборудования по защите информации; • Иметь опыт установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;	
ПК 3.3. Обеспечение безопасного администрирования многоканальных телекоммуникационных систем и информационно-коммуникационных сетей связи.	• Иметь опыт конфигурирования автоматизированных систем и информационно-коммуникационных сетей; • Иметь опыт защиты баз данных; • Иметь опыт организации защиты в различных операционных системах и средах; • Иметь опыт шифрования информации	

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.	- демонстрация интереса к будущей профессии	Текущий контроль в форме: -защиты лабораторных занятий; - наблюдения преподавателя за выполнением конкретного задания; - аудирование - зачеты по учебной практике и по каждому из МДК; -квалификационный экзамен по профессиональному модулю
ОК 2. Организовывать собственную деятельность, определять методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач в области телекоммуникаций, а также технической эксплуатации и монтажа систем передачи - 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 в области телекоммуникаций	
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	-эффективный поиск необходимой информации в технической документации; - использование различных источников информации, включая web-ресурсы.	
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- работа с оборудованием телекоммуникаций; - работа со специализированным ПО.	
ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- взаимодействие с обучающимися, преподавателями, мастерами в ходе обучения	
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат	- самоанализ и коррекция результатов собственной работы и работы членов команды.	

выполнения заданий		
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- организация самостоятельного обучения при изучении профессионального модуля;	
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- умение ориентироваться в условиях смены технологий в области телекоммуникаций	

ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ РАБОЧЕЙ ПРОГРАММЫ

№	Изменения и дополнения	Подпись, дата.

Рабочая программа обсуждена на заседании кафедры

Протокол № _____ от «_____»_____20___г.

Заведующий кафедрой_____/_____/

Рабочая программа обсуждена на заседании кафедры

Протокол № _____ от «_____»_____20___г.

Заведующий кафедрой_____/_____/

Рабочая программа обсуждена на заседании кафедры

Протокол № _____ от «_____»_____20___г.

Заведующий кафедрой_____/_____/

Рабочая программа обсуждена на заседании кафедры

Протокол № _____ от «_____»_____20___г.

Заведующий кафедрой_____/_____/

Федеральное агентство связи

Бурятский институт инфокоммуникаций Федеральное государственное бюджетное образовательное учреждение Высшего образования «Сибирский государственный университет телекоммуникаций и информатики» в г. Улан-Удэ

Рассмотрена и одобрена
на заседании кафедры ТКС

зав. кафедрой_____/ Нестеров А. С./

«____» _____ 20_____г.

УТВЕРЖДАЮ

Заместитель директора по УНР

_____/Батурина Т.Г./

«____» _____ 20____ г.

ПРОГРАММА ПМ03
Обеспечения информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи

УП 03.01. Технология применения комплексной системы защиты информации

Форма обучения: очная
Квалификация: техник
Специальность: 11.02.09 «Многоканальные телекоммуникационные системы»
Факультет: Телекоммуникаций
Курс: 2

Объем в часах: 36 ч.

Учебная – 36 ч.

Формы и сроки контроля:

Диф. зачет - 4 семестр

Программу разработал: Поздняков П.В. /_____/
Ф.И.О. подпись

Улан-Удэ, 2017 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРАКТИКИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 Обеспечения информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи

1.2. Область применения программы

Программа профессионального модуля (далее - программа) – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО **11.02.09 Многоканальные телекоммуникационные системы**(базовой подготовки) в части освоения основного вида профессиональной деятельности (ВПД): **Обеспечения информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи**и соответствующих профессиональных компетенций (ПК):

ПК 3.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.

ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. Управлять данными телекоммуникационных систем.

ПК 3.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.

Программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке в области телекоммуникаций при наличииосреднего (полного) общего образования, опыт работы не требуется.

Программа профессионального модуля может быть использована при повышении квалификации и переподготовке работников связи при наличии профессионального образования.

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

С целью овладения указанным видом профессиональной деятельности исоответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- выявления каналов утечки информации;
- определения необходимых средств защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы;
- установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
- конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
- защиты баз данных;

- организации защиты в различных операционных системах и средах;
- шифрования информации;

уметь:

- 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

1.2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Обеспечения информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи
ПК 3.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению. Управлять данными телекоммуникационных систем
ПК 3.3	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, оцениватьих 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 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.

1.3. Этапы практики

Учебная:

- срок проведения –4 семестр, объем – 36ч; итог практики –**дифференцированный зачет**

1.4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО УЧЕБНОЙ ПРАКТИКЕ (практика по профилю специальности)

Учебная практика (по профилю специальности) ПМ.03

МДК 03.02
Виды работ:

1. Настройка роутера
2. Настойка Watchdog (сторожевой таймер)
3. Настройка Filter
4. Настройка filter с использованием Addresslists
5. Настройка Layer7 filter
6. Расширенная настройка фильтрации пакетов
7. Настройка VPN (PPTP)
8. Настройка VPN (L2TP)
9. Настройка маркировки соединения
10. Настройка резервного канала

Тематический план

УП.03.01.Учебная практика

№п/п	Задание по программе, компетенции	Количество часов	Содержание темы, индивидуальные задания
1	Настройка роутера, ПК 2.1	2	DHCP, PPPoE
2	Настойка Watchdog, ПК 3.1, ПК 3.2	4	Watchdog, SysLog Watcher
3	Настройка Filter, ПК 3.1, ПК 3.2	4	Filtering
4	Настройка filter с использованием Addresslists, ПК 3.1, ПК 3.3	4	Address lists
5	Настройка Layer7 filter, ПК 3.1, ПК 3.3	2	Layer7 filter
6	Расширенная настройка фильтрации пакетов ПК 3.1, ПК 3.2	4	Filtering
7	Настройка VPN (PPTP),	4	PPTP

	ПК 3.1, ПК 3.3		
8	Настройка VPN (L2TP), ПК 3.1, ПК 3.3	4	L2TP
9	Настройка маркировки соединения, ПК 3.1	4	Mangle
10	Настройка резервного канала, ПК 3.1, ПК 3.3	4	Routes
Итого		**36 ч**	

Ведомости результатов практики (учебной) по профессиональному модулю

УП 03.01 Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи

Ф.И.О студента	**Оценки члена аттестационной комиссии по практике (оценка положительная – 1/ отрицательная – 0) по ОПОР**					
	ПК 3.1		ПК 3.2		ПК 3.3	
	ОПОР 1.1	ОПОР 1.2	ОПОР 2.1	ОПОР 2.2	ОПОР 3.1	ОПОР 3.2

«_____»_____ 20___г. Подпись руководителя практики:

_____ /ФИО, должность/