Федеральное агентство связи
Уральский технический институт связи и информатики (филиал)
ФГБОУ ВО «Сибирский государственный университет
телекоммуникаций и информатики» в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УРАЛЬСКИЙ ТЕХНИЧЕСКИЙ ИНСТИТУТ СВЯЗИ И ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор УрТИСИ СибГУТИ
_____ Е.А. Субботин
«29» 06 2016 г.

Рабочая программа профессионального модуля

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ

для специальности:
11.02.09 «Многоканальные телекоммуникационные системы»

Екатеринбург
2016

Федеральное агентство связи
Уральский технический институт связи и информатики (филиал)
ФГБОУ ВО «Сибирский государственный университет
телекоммуникаций и информатики» в г. Екатеринбурге
(УрТИСИ СибГУТИ)

УТВЕРЖДАЮ
Директор УрТИСИ СибГУТИ
_____ Е.А. Субботин
«____» _____ 20__ г.

Рабочая программа профессионального модуля

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МНОГОКАНАЛЬНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ ЭЛЕКТРОСВЯЗИ

для специальности:
11.02.09 «Многоканальные телекоммуникационные системы»

Екатеринбург
2016

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол №10 от 29.06.2016
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано
Заместитель директора
по учебно-методической работе
_____ Е.А. Минина

Автор: Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Рецензент: Татаркина О.А. - начальник станционного участка Екатеринбургского филиала ПАО «Ростелеком»

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 11.02.09 «Многоканальные телекоммуникационные системы» (утвержденного приказом Минобрнауки РФ от 28 июля 2014г. №811, зарегистрированного в Минюсте РФ 19 августа 2014г. №33637).

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано
Заместитель директора
по учебно-методической работе
_____ Е.А. Минина

Автор: Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Рецензент: Татаркина О.А. - начальник станционного участка Екатеринбургского филиала ПАО «Ростелеком»

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 11.02.09 «Многоканальные телекоммуникационные системы» (утвержденного приказом Минобрнауки РФ от 28 июля 2014г. №811, зарегистрированного в Минюсте РФ 19 августа 2014г. №33637).

ЛИСТ СОГЛАСОВАНИЯ

Рабочей программы профессионального модуля
ПМ.03 «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи»
и оценочных средств
для специальности 11.02.09 «Многоканальные телекоммуникационные системы» (базовой подготовки)

Эксперт(ы) (рецензент(ы)) от профильного предприятия отрасли:	ФИО	Заключение о согласовании программы	Подпись, дата, М.П
Начальник станционного участка Екатеринбургского филиала ПАО «Ростелеком»	Татаркина Ольга Александровна	согласовано	
(место работы и должность)			
Дополнения и предложения работодателя			

Подпись

Рассмотрено на заседании цикловой комиссии МТС
и рекомендовано для учебных занятий в 2017 - 2018 учебном году.
Протокол №10 от 29.06.2017
Председатель цикловой комиссии _____

Рассмотрено на заседании цикловой комиссии МТС
и рекомендовано для учебных занятий в 2018 - 2019 учебном году.
Протокол №11 от 15.06.2018
Председатель цикловой комиссии _____

Рассмотрено на заседании цикловой комиссии МТС
и рекомендовано для учебных занятий в 2019 - 2020 учебном году.
Протокол №13 от 28.06.2019
Председатель цикловой комиссии _____

2020 - 2021 учебный год
Протокол №1 от 01.09.2020

2021 - 2021 учебный год
Протокол №1 от 03.09.2021

Рассмотрено на заседании цикловой комиссии _____
и рекомендовано для учебных занятий в _____ учебном году.
Протокол ___ от _____
Председатель цикловой комиссии _____

Рассмотрено на заседании цикловой комиссии _____
и рекомендовано для учебных занятий в _____ учебном году.
Протокол ___ от _____
Председатель цикловой комиссии _____

Рассмотрено на заседании цикловой комиссии _____
и рекомендовано для учебных занятий в _____ учебном году.
Протокол ___ от _____
Председатель цикловой комиссии _____

СОДЕРЖАНИЕ

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1 Область применения программы

Рабочая программа профессионального модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» 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): «Обеспечение 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.

1.2 Цели и задачи профессионального модуля - требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими 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 Рекомендуемое количество часов на освоение программы профессионального модуля:

Всего - ***198 часов***, в том числе:

- максимальной учебной нагрузки обучающегося - ***144 часа***, включая:
  - обязательной аудиторной учебной нагрузки обучающегося - ***96 часов***;
  - самостоятельной работы обучающегося - ***36 часов***;
  - консультаций обучающегося - ***12 часов***;
- учебной практики и производственной практики (по профилю специальности) - ***54 часа***.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) «Обеспечение 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 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.
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 профессионального модуля

Коды проф. компетенций	Наименование разделов профессионального модуля	Всего часов (макс. учебная нагрузка и практики)	Объем времени, отведенный на освоение междисциплинарного курса						Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося		Консультации	Учебная, часов	Производственная (по профилю специальности), часов
			Всего, часов	в т.ч. лаб. работы и практ. 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	11
ПК 3.1, ПК 3.2	Раздел 1 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи	72	36	18	-	12	-	6	18	-
ПК 3.2, ПК 3.3	Раздел 2 Технология применения комплексной системы защиты информации	108	60	30	-	24	-	6	18	-
ПК 3.1, ПК 3.2, ПК 3.3	Производственная практика (по профилю специальности), часов	18								18
	Всего:	198	96	48	-	36	-	12	36	18

3.2 Содержание обучения по профессиональному модулю

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Уровень освоения	Осваиваемые компетенции	Литература для выполнения заданий самостоятельной работы обучающихся
1	2	3	4	5	6
Раздел 1 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи		**72**			
МДК.03.01 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи		**72**			
Тема 1 Основы информационной безопасности	1 Понятие информационной безопасности, характеристика ее составляющих. Место информационной безопасности в системе национальной безопасности. Концептуальная модель защиты информации. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1, 3], Интернет-ресурсы
	2 Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. Виды уязвимости информации и формы ее проявления. Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне).	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	3 Уровни информационной безопасности - законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	Практические занятия: 1 Анализ угроз безопасности персональных данных при их обработке в информационных системах. 2 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.	 2 2		ОК 2, ОК 3, ОК 4, ОК 6, ОК 7, ПК 3.1, ПК 3.2	[1,2,3]

	3 Изучение особенностей аттестации помещений по требованиям безопасности информации. 4,5 Составление комплекта документации для лицензирования работ и услуг в области защиты информации (ФСТЭК). 6 Анализ информационных ресурсов, циркулирующих в организации.	2 4 2			
	Самостоятельная работа обучающихся: 1 Конспектирование учебного материала по теме. 2 Подготовка ответов на контрольные вопросы практических занятий.	 2 2		ОК 2, ОК 4, ОК 5, ОК 8	[1,2,4], Интернет-ресурсы
Тема 2 Правовое обеспечение информационной безопасности	1 Информация как объект права. Нормативно-правовые основы информационной безопасности в РФ. Законодательно-нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации. Конституционные гарантии прав граждан в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	2 Система защиты государственной тайны, правовой режим защиты государственной тайны. Лицензирование и сертификация в области защиты информации. Стандартизация информационной безопасности.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	Самостоятельная работа обучающихся: 1 Конспектирование учебного материала по теме. 2 Разработка рефератов по стандартам безопасности, статьям Конституции РФ, статьям Гражданского и Уголовного кодексов в области информационной безопасности.	 2 2		ОК 2, ОК 4, ОК 5, ОК 8	[1,2,4], Интернет-ресурсы
Тема 3 Организационное обеспечение информационной безопасности	1 Сущность и сферы действия организационной защиты информации. Механизмы обеспечения информационной безопасности. Разработка политики безопасности.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	2 Проведение анализа угроз и расчета рисков в области информационной безопасности.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,3,4], Интернет-ресурсы

	3 Выбор механизмов и средств обеспечения информационной безопасности. Модели защиты информационных систем.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,5], Интернет ресурсы
	4 Правила организации работ подразделений защиты информации. Разработка инструкций по работе со средствами защиты. Организация работы персонала с конфиденциальной информацией.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,3,4], Интернет-ресурсы
	Практические занятия: 7 Анализ программно-технических средств, используемых в организации. 8 Анализ программно-технических средств предприятия 9 Анализ защищаемого помещения и каналов утечки информации.	 2 2 2		ОК 2, ОК 3, ОК 4, ОК 6, ОК 7, ПК 3.1, ПК 3.2	[1,3,4]
	Самостоятельная работа обучающихся: 1 Конспектирование учебного материала по теме. 2 Подготовка ответов на контрольные вопросы практических занятий.	 2 2		ОК 2, ОК 4, ОК 5, ОК 8	[1,3,4], Интернет-ресурсы
Консультации:		**6**			
Учебная практика		**18**			
Виды работ: 1 Оценка информационной безопасности объектов на законодательном, административном, процедурном и программно-техническом уровнях. 2 Правовая оценка действий злоумышленника при создании угроз информационной безопасности. 3 Способы и методы организации защиты от угроз в сетях связи. 4 Организация инженерно-технической безопасности от угроз. 5 Кадровая безопасность.				ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 7, ОК 8, ОК 9, ПК 3.1, ПК 3.2	[1,2,3,4], Интернет ресурсы
Раздел 2 Технология применения комплексной системы защиты информации		**108**			
МДК 03.02 Технология применения комплексной системы защиты информации		**108**			
Тема 1 Программно-аппаратные средства защиты информации	1 Информационная безопасность в многоканальных телекоммуникационных системах и сетях электросвязи.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	2 Структурные схемы систем защиты информации в типовых информационных системах. Показатели защищенности многоканальных телекоммуникационных систем.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы

	3 Сервисы, обеспечивающие информационную безопасность в многоканальных телекоммуникационных системах и сетях электросвязи: ограничение физического доступа к автоматизированным системам.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,3], Интернет-ресурсы
	4 Идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит).	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	5 Криптографическая защита; контроль целостности; управление политиками безопасности.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	6 Уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,4], Интернет-ресурсы
	7 Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,4], Интернет-ресурсы
	8 Антивирусные программы и комплексы. Построение систем антивирусной защиты телекоммуникационных систем и сетей.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,3,4], Интернет-ресурсы
	9 Построение систем антивирусной защиты телекоммуникационных систем и сетей.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,3,4], Интернет-ресурсы
	Практические занятия: 1 Методы аутентификации, использующие пароли. Настройка параметров аутентификации Windows 7 (XP). 2 Назначение прав пользователей при произвольном управлении доступом в Windows 7 (XP). 3 Настройка защитных механизмов ОС Windows 7 (XP). 4 Установка и настройка программного антивирусного комплекса. 5 Установка и настройка программно-аппаратных антивирусных средств. 6 Установка и настройка межсетевого экрана.	 2 2 2 2 2 2		ОК 2, ОК 3, ОК 4, ОК 6, ОК 7, ПК 3.2, ПК 3.3	[1,2,3,4], Интернет-ресурсы
	Самостоятельная работа обучающихся: 1 Конспектирование учебного материала по теме.	 4		ОК 2, ОК 4, ОК 5, ОК 8	[1,2,3,4], Интернет-ресурсы

	2 Подготовка ответов на контрольные вопросы практических занятий.	8			
Тема 2 Администрирование телекоммуникационных систем и сетей связи	1 Технологии защиты данных. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография).	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,3,4], Интернет-ресурсы
	2 Различные технологии аутентификации. Технологии защиты межсетевого обмена данных.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,3,4], Интернет-ресурсы
	3 Технология обеспечения безопасности сетевых операционных систем. Основы технологии виртуальных защищенных сетей VPN.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2,3,4], Интернет-ресурсы
	4 Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак).	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2], Интернет-ресурсы
	5 Требования по защите от несанкционированного доступа.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2], Интернет-ресурсы
	6 Технические средства обеспечения безопасности многоканальных телекоммуникационных систем.	2	2	ОК 1, ОК 2, ОК 5, ОК 6, ОК 8, ОК 9	[1,2], Интернет-ресурсы
	Практические занятия: 7 Шифрование методами перестановки и простой замены. 8 Шифрующая файловая система EFS и управление сертификатами в Windows 7 (XP). 9 Установка и настройка программных средств защиты телекоммуникационных систем и сетей электросвязи. 10,11 Аппаратные средства защиты информации. 12 Установка и настройка камер видеонаблюдения. 13 Установка и настройка датчиков контроля вскрытия линейно-кабельных сооружений и устройств. 14 Установка и настройка датчиков тревожной сигнализации. 15 Разработка технического задания на создание защиты информационной системы.	 2 2 2 4 2 2 2 2		ОК 2, ОК 3, ОК 4, ОК 6, ОК 7, ПК 3.2, ПК 3.3	[1,2,4]
	Самостоятельная работа обучающихся: 1 Конспектирование учебного материала по теме.	 4		ОК 2, ОК 4, ОК 5, ОК 8	[1,2,3,4], Интернет ресурсы

	2 Подготовка ответов на контрольные вопросы практических занятий.	8			
Консультации		**6**			
Учебная практика		**18**			
Виды работ: 1 Аппаратные средства защиты информации. 2 Идентификация и аутентификация. 3 Защитные механизмы операционных систем Windows 7, Linux, Unix. 4 Антивирусные программные и программно-аппаратные комплексы. 5 Межсетевые экраны. 6 Совокупность процедур и правил криптографических преобразований. 7 Зашифрование информации. Расшифрование информации.				ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 7, ОК 8, ОК 9, ОК 3.2, ПК 3.3	[1,2,3,4], Интернет-ресурсы
Производственная практика (по профилю специальности)		**18**			
Виды работ: 1 Установка, настройка специализированного оборудования по защите информации. 2 Выявление возможных атак на автоматизированные системы. 3 Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей. 4 Конфигурирование автоматизированных систем и информационно -коммуникационных сетей. 5 Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей. 6 Организации защиты в различных операционных системах и средах.				ОК 1, ОК 2, ОК 3, ОК 4, ОК 5, ОК 6, ОК 7, ОК 8, ОК 9, ПК 3.1, ПК 3.2, ПК 3.3	
Всего		**198**			

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (узнавание ранее изученных объектов, свойств);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Реализация рабочей программы профессионального модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» предполагает наличие учебных лабораторий:

МДК.03.01 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи	Лаборатория информационной безопасности №312 УК №1	*Оборудование учебной лаборатории:* Количество мест – 15. Офисная мебель. Доска аудиторная белая под маркер 1500*1000 1 шт. *Технические средства обучения:* Компьютер Intel Celeron 430 с клавиатурой и мышью 15 шт. Монитор LCD 17" Proview MA-782KC (8 мс) серебристый/черный 15 шт. Монитор ЖК 17 Acer AL 1721M 1 шт.
МДК.03.02 Технология применения комплексной системы защиты информации	Лаборатория информационной безопасности №312 УК №1	*Оборудование учебной лаборатории:* Количество мест – 15. Офисная мебель. Доска аудиторная белая под маркер 1500*1000 1 шт. *Технические средства обучения:* Компьютер Intel Celeron 430 с клавиатурой и мышью 15 шт. Монитор LCD 17" Proview MA-782KC (8 мс) серебристый/черный 15 шт. Монитор ЖК 17 Acer AL 1721M 1 шт.
Учебная практика	Лаборатория информационной безопасности №312 УК №1	*Оборудование учебной лаборатории:* Количество мест – 15. Офисная мебель. Доска аудиторная белая под маркер 1500*1000 1 шт. *Технические средства обучения:* Компьютер Intel Celeron 430 с клавиатурой и мышью 15 шт. Монитор LCD 17" Proview MA-782KC (8 мс) серебристый/черный 15 шт. Монитор ЖК 17 Acer AL 1721M 1 шт.

4.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы, Интернет-ресурсов:

МДК.03.01 Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи

Основные источники:

1 Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 266 c. - 978-5-94774-821-5. - Режим доступа: http://www.iprbookshop.ru/52209.htm.

2 Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / Нестеров С.А. - Электрон. текстовые данные. - СПб. : Санкт-Петербургский политехнический университет Петра Великого, 2014. - 322 c. - 978-5-7422-4331-1. - Режим доступа: http://www.iprbookshop.ru/43960.html.

3 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

Дополнительные источники:

4 Бахаров Л.Е. Информационная безопасность и защита информации. - Москва: Издательский дом МИСиС 2015 г.- 43 с. - Электронное издание. - Режим доступа: https://ibooks.ru.

5 Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 424 c. - 2227-8397. - Режим доступа: http://www.iprbookshop.ru/52161.html.

6 Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Электрон. текстовые данные. - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. - 113 c. - 978-5-9585-0603-3. - Режим доступа: http://www.iprbookshop.ru/.

7 Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. - Электрон. текстовые данные. - Саратов:АйПиЭрБукс, 2015.- 326 c. - 978-5-906-17271-6. - Режим доступа: http://www.iprbookshop.ru/33857.html.

МДК.03.02 Технология применения комплексной системы защиты информации

Основные источники:

1 Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс] : научно-техническое издание / А.И. Астайкин [и др.]. - Электрон. текстовые данные. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. - 224 c. - 978-5-9515-0305-3. - Режим доступа: http://www.iprbookshop.ru/60959.html.

2 Скрипник Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. - Электрон. текстовые данные. - М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. - 424 c. - 2227-8397. - Режим доступа: http://www.iprbookshop.ru/52161.html.

Дополнительные источники:

3 Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. - Электрон. текстовые данные. - Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. - 113 c. - 978-5-9585-0603-3. - Режим доступа: http://www.iprbookshop.ru/.

4 Петров С.В. Информационная безопасность [Электронный ресурс] : учебное пособие / С.В. Петров, П.А. Кисляков. - Электрон. текстовые данные.- Саратов:АйПиЭрБукс,2015.- 326 c. - 978-5-906-17271-6. - Режим доступа: http://www.iprbookshop.ru/33857.html.

Интернет-ресурсы:

1 http://www.ISO 27000.ru - Международные стандарты управления информационной безопасностью.

2 http://www. info-ispdn.ru - Национальные стандарты Российской Федерации в области защиты информации.

3 http://www.cbi-info.ru/common - ISO 15408 - Общие критерии оценки безопасности информационных технологий.

4 http://www.fsb.ru - Сайт Федеральной Службы Безопасности.

5 http://www.fstec.ru - Сайт ФСТЭК России.

4.3 Общие требования к организации образовательного процесса

В целях реализации компетентностного подхода в освоении программы профессионального модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» учебные занятия следует проводить в лабораториях и кабинетах, оснащенных необходимым учебным, методическим, информационным и программным обеспечением.

В преподавании необходимо использовать активные и интерактивные формы проведения занятий.

Изучению профессионального модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» должно предшествовать изучение общепрофессиональных дисциплин профессионального цикла:

1) Теория электрических цепей;
2) Электронная техника;
3) Теория электросвязи;
4) Вычислительная техника;
5) Электрорадиоизмерения;
6) Основы телекоммуникаций;

7) Энергоснабжение телекоммуникационных систем;

8) Безопасность жизнедеятельности.

Реализация программы профессионального модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» предполагает обязательную учебную практику и производственную практику (по профилю специальности).

Обязательным условием допуска к учебной практике является освоение обучающимися соответствующих междисциплинарных курсов (МДК) данного профессионального модуля.

Учебная практика должна обеспечивать практико-ориентированную подготовку обучающихся.

Допуском к производственной практике (по профилю специальности) в рамках профессионального модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» является освоение обучающимися следующих МДК:

1) Технология применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи;

2) Технология применения комплексной системы защиты информации и учебной практики.

4.4 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарным курсам:

- наличие высшего образования, соответствующего профилю модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи» и специальности 11.02.09 «Многоканальные телекоммуникационные системы».

Требования к квалификации педагогических (инженерно-педагогических) кадров, осуществляющих руководство практикой:

- дипломированные специалисты - преподаватели междисциплинарных курсов;

- дипломированные специалисты профильных организаций.

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Формы и методы контроля и оценки результатов обучения, позволяющие проверять у обучающихся сформированность профессиональных компетенций:

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	- четкое понимание проблем информационной безопасности в сфере телекоммуникаций; - грамотное выявление, классификация и анализ угроз информационной безопасности и формы их проявления; - выбор механизмов и средств обеспечения информационной безопасности программных и программно-аппаратных; - грамотное оформление документации для лицензирования работ в области информационной безопасности; - разработка политики в области информационной безопасности.	Текущий контроль в форме: - защиты практических занятий; - исследовательско-поисковый характер работы по тематике модуля с использованием Internet. Зачеты по учебной практике, по производственной практике (по профилю специальности). Дифференцированные зачеты по каждому МДК. Квалификационный экзамен по профессиональному модулю.
Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать реко - мендации по их устранению	- расчет рисков в области информационной безопасности и выдача рекомендаций по их устранению; - владение сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи; - владение технологией аутентификации; - обеспечение технологии защиты межсетевого обмена данными; - построение системы антивирусной защиты систем телекоммуникационных систем.	
Обеспечивать безопасное администрирование телекоммуникационных систем и сетей связи	- 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, позволяющие проверять у обучающихся развитие общих компетенций и обеспечивающих их умений:

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 практических занятий; - электронного тестирования. Зачеты по учебной и производственной практикам. Зачеты по каждому из разделов профессионального модуля. Комплексный экзамен по профессиональному модулю.
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 направляющих систем; - оценка эффективности и качества выполнения.	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- решение стандартных и нестандартных профессиональных задач в области телекоммуникаций.	
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.	
Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- владение технологиями эксплуатации оборудования информационно-коммуникационных сетей.	
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	- сотрудничество с коллегами, руководством и мотивированное общение с потребителями.	

Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	- анализ результатов деятельности команды и собственной работы.	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- организация самостоятельного обучения при изучении профессионального модуля; - планирование повышения квалификации.	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- анализ инновационных технологий в области телекоммуникаций.	

Регистрация изменений в рабочей программе

№ п/п	Учебный год	Содержание изменений	Препода-ватель	Решение цикловой комиссии (№ протокола, дата, подпись ПЦК)