Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

УТВЕРЖДАЮ
Генеральный директор
ПАО «Интелтех»

М.В. Винокур
«28» ноября 2023 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

СПЕЦИАЛИСТОВ СВЯЗИ – АДМИНИСТРАТОРОВ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

(ДОПОЛНИТЕЛЬНАЯ К ВЫСШЕМУ ПРОФЕССИОНАЛЬНОМУ ОБРАЗОВАНИЮ)

Рассмотрена на заседании
Научно-технического совета
ПАО «Интелтех».
Протокол № 14-23
от «27» апреля 2023 г.

Санкт-Петербург
2023

Настоящая дополнительная профессиональная программа профессиональной переподготовки специалистов связи – администраторов инфокоммуникационных сетей разработана на основании Федерального закона Российской Федерации от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» и приказа Министерства образования и науки Российской Федерации от 01 июля 2013 года № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Дополнительная профессиональная программа профессиональной переподготовки специалистов связи – администраторов инфокоммуникационных сетей реализуется в Учебном центре дополнительного профессионального образования Публичного акционерного общества «Информационные телекоммуникационные технологии» (ПАО «Интелтех»).

Дополнительная профессиональная программа обсуждена на заседании Научно-технического совета ПАО «Интелтех» « 27 » апреля 2023 г. протокол № 14-23.

С о с т а в и т е л и:

Будко Павел Александрович – ученый секретарь ПАО «Интелтех»,
доктор технических наук, профессор

Курносов Валерий Игоревич – главный специалист ПАО «Интелтех»,
доктор технических наук, профессор,
заслуженный работник связи Российской Федерации

Р е ц е н з е н т:

Яшин Александр Иванович – профессор кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ»,доктор технических наук, профессор, заслуженный деятель науки Российской Федерации

_____

1. Цель реализации дополнительной профессиональной программы

Целью реализации дополнительной профессиональной программы является осуществление образовательной деятельности, направленной на совершенствование и (или) получение новых компетенций, необходимых для профессиональной деятельности специалистов связи по применению военной электронно-вычислительной техники, и повышение их профессионального уровня в рамках имеющейся квалификации.

2. Планируемые результаты обучения

2.1. Перечень профессиональных компетенций в рамках имеющейся квалификации, качественное изменение которых осуществляется при освоении дополнительной профессиональной программы:

способен обеспечивать эффективное использование эксплуатационных свойств и технических возможностей электронно-вычислительной техники, комплексов средств автоматизации (КСА) в различных условиях обстановки;

способен применять технические, программные и информационные средства сетевых и информационных технологий в АСУ общего и специального назначения.

2.2. Качественное изменение профессиональных компетенций достигается следующими уровнями обученности:

иметь представление:

о назначении и принципах построения глобальных и локальных вычислительных сетей;

об обеспечении безопасности личного состава при эксплуатации КСА;
о концептуальных основах защиты информации в АСУ общего и специального назначения;

о перспективах развития информационных технологий и их применения в системах управления телекоммуникационными сетями и системами общего и специального назначения;

знать:

архитектуру, протоколы, базовые средства вычислительных сетей;

характеристики и возможности технических средств построения КСА;

возможности базовых средств новых информационных технологий;

основы построения информационных систем и проектирования баз данных;

содержание и организацию технической эксплуатации, ввод в эксплуатацию и обслуживания КСА общего и специального назначения;

содержание и организацию защиты информации в АСУ общего и специального назначения;

уметь:

применять технические и программные средства сетевых и информационных технологий в АСУ общего и специального назначения;

использовать системы управления базами данных для администрирования и актуализации информационных ресурсов;

применять средства конфигурирования КСА на базе локальных вычислительных сетей (ЛВС) и персональных ЭВМ, обеспечивать инсталляцию, настройку и сопровождение программного обеспечения КСА;

выполнять ввод в эксплуатацию и обслуживание КСА;

применять средства защиты информации в КСА общего и специального назначения.

3. Итоговая аттестация

Освоение дополнительной профессиональной программы завершается обязательной итоговой аттестацией в виде зачёта с оценкой.

Для проведения итоговой аттестации создается аттестационная комиссия по дополнительной профессиональной программе, состав которой утверждается генеральным директором ПАО «Интелтех».

Председатель аттестационной комиссии назначается приказом генерального директора ПАО «Интелтех»из числа его заместителей.

В состав аттестационной комиссии по согласованию включаются представители Заказчика.

3.1. Перечень вопросов и оценочных средств к итоговой аттестации

1) Назначение и возможности вычислительных сетей в автоматизированных системах управления общего и спциального назначения.
2) Характеристики и возможности технических средств построения КСА.
3) Концепция локальных вычислительных сетей.
4) Архитектура и типы структур локальных вычислительных сетей.
5) Базовые протоколы локальных вычислительных сетей.
6) Технологии построения локальных вычислительных сетей.
7) Базовые средства локальных вычислительных сетей.
8) Назначение и классификация сетевых операционных систем.
9) Состав и функции сетевой операционной системы.
10) Возможности базовых средств новых информационных технологий.
11) Геоинформационные технологии и средства построения геоинформационных систем.
12) Основы построения информационных систем.
13) Основы проектирования баз данных.
14) Системы управления базами данных.
15) Модели данных информационных систем.
16) Построение и программное обеспечение системы обмена информацией в электронном виде.
17) Назначение и структура службы доменных имен.
18) Системы электронного документооборота (СЭД). Назначение и состав СЭД.
19) Содержание и организация технической эксплуатации КСА общего и специального назначения.
20) Характеристика мероприятий ввода в эксплуатацию и обслуживания КСА общего и специального назначения.

21) Обеспечение безопасности обслуживающего персонала при эксплуатации КСА.

22) Средства сетевого планирования мероприятий.

23) Концептуальных основы защиты информации в АСУ общего и специального назначения.

24) Методы и средства обеспечения безопасности информации в автоматизированных системах.

25) Концепция защиты от несанкционированного доступа к информации в автоматизированных системах общего и специального назначения.

26) Модели, методы и средства защиты от несанкционированного доступа.

27) Компьютерные вирусы и программные закладки.

28) Защита от компьютерных вирусов и программных закладок.

29) Программные атаки и способы защиты от них.

30) Содержание и организация защиты информации в АСУ общего и специального назначения.

31) Порядок разработки документов по защите информации от НСД.

4. Организационно-педагогические условия

4.1. Кадровое обеспечение учебного процесса.

Для реализации программы привлекать наиболее опытный научно-педагогический состав ПАО «Интелтех», не менее 70% которого должны иметь ученую степень и (или) ученое звание.

Для проведения занятий со слушателями могут привлекаться ведущие ученые и специалисты ПАО «Интелтех», других вузов и научно-исследовательских учреждений.

4.2. Требования к информационно-методическому обеспечению учебного процесса.

Реализация дополнительной профессиональной программы должна обеспечиваться библиотечными и учебно-информационными фондами ПАО «Интелтех».

Программа должна быть обеспечена учебной (учебно-методической) литературой и электронными учебными пособиями по всем видам учебных занятий и всему объёму самостоятельной работы слушателей, нормативно-правовыми документами. Требуемая обеспеченность учебно-методической литературой, соответствующей по содержанию программе – не менее одного экземпляра на двух слушателей.

При реализации программы предусмотреть:

предоставление каждому слушателю возможности регулярного пользования программно-аппаратными средствами информатизации, обеспечивающими доступ к ресурсам локальной сети Интернет;

наличие сведений о других информационных базах (отечественная и зарубежная научно-педагогическая периодика, архивы данных и т. п.) и обеспечение условий для доступа к ним.

Библиотечный фонд должен быть укомплектован печатными и (или) электронными изданиями, основной учебной и научной литературой, изданными за последние 3 года, дополнительной литературой, изданной за последние 5 лет, действующей на текущий период подготовки нормативной и справочной литературой.

4.3. Требования к материально-техническому обеспечению учебного процесса.

ПАО «Интелтех», на базе которого реализуется программа, должна располагать учебно-материальной базой, соответствующей действующим санитарно-техническим нормам и обеспечивающей проведение всех видов занятий со слушателями в соответствии с учебным планом. Реализация программы требует наличия лекционной аудитории, оборудованной мультимедийными средствами отображения информации с количеством посадочных мест не менее 15. Для обеспечения проведения практических видов занятий и самостоятельной подготовки обучающиеся должны быть обеспечены средствами вычислительной техники, объединёнными в локальную вычислительную сеть, из расчета: одна персональная ЭВМ на одного-двух слушателей.

5. Организация входного контроля.

5.1. Цель и задачи входного контроля.

Входной контроль со слушателями, обучающимися по дополнительной профессиональной программе профессиональной переподготовки проводится с целью определения реального предварительного уровня знаний поступающих на курс обучения в Учебный центр и формирования объективных исходных данных для организации образовательного процесса по специальности подготовки.

Основными задачами входного контроля являются:

оценка уровня подготовленности слушателей к обучению по профессиональной программе профессиональной переподготовки;

разработка рекомендаций по повышению эффективности образовательной деятельности по дополнительной профессиональной программе профессиональной переподготовки в соответствии с базовым уровнем подготовки слушателей;

учет реального уровня подготовки слушателей при организации образовательной деятельности по дополнительной профессиональной программе профессиональной переподготовки.

5.2. Порядок проведения входного контроля.

Входной контроль слушателей проводится в часы самоподготовки в начале обучения по дополнительной профессиональной программе профессиональной переподготовки.

Время на проведение входного контроля – до 2 академических часов.

Для проведения входного контроля в Учебном центре разрабатываются методические рекомендации и перечень вопросов для проведения входного контроля.

5.3. Перечень программных вопросов для проведения входного контроля слушателей, обучающихся по дополнительной профессиональной программе профессиональной переподготовки.

1) Система руководящих документов по работе должностных лиц управления обеспечением автоматизации на узлах (предприятиях) связи.

2) Общая характеристика глобальных вычислительных сетей.

3) Общая характеристика локальных вычислительных сетей.

4) Понятия архитектуры, логической и физической структуры вычислительных сетей.

5) Характеристика основных технических средств автоматизации, находящихся на оснащении узла (предприятия) связи.

6) Стандарты для локальных вычислительных сетей.

7) Общая характеристика современных информационных технологий.

8) Характеристика автоматизированных информационных систем.

9) Виды обеспечения автоматизированных систем управления.

10) Характеристика системы обмена информацией в электронном виде в системах общего назначения.

11) Основы защиты информации в автоматизированных системах управления (АСУ) общего назначения.

12) Системы счисления. Перевод чисел из одной системы счисления в другую.

13) Система адресации в вычислительных сетях. Типы адресов.

14) Современная система адресации в вычислительных сетях.

Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

УЧЕБНЫЙ ПЛАН

ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

СПЕЦИАЛИСТОВ СВЯЗИ – АДМИНИСТРАТОРОВ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ

(ДОПОЛНИТЕЛЬНАЯ К ВЫСШЕМУ ПРОФЕССИОНАЛЬНОМУ ОБРАЗОВАНИЮ)

Санкт-Петербург
2023

а) Сводные данные по бюджету учебного времени

Трудоёмкость программы			Распределение учебного времени (количество часов)			
Всего учебных недель	Количество зачётных единиц	Учебное время	Аудиторная работа	Самостоятельная работа	Стажировки (практики)	Итоговая (промежуточная) аттестация
10	3	572	400	180	-	8(18)

б) План учебного процесса

№ пп	Наименование модулей, учебных дисциплин	Всего часов на освоение учебного материала	Часы занятий с препо-давателем	Распределение учебного времени				Итоговый контроль		
				Лекций	Практи-ческие занятия	Груп-повые занятия	Время на самостоя-тельную работу	Зачет с оце-нкой	Зачет без оцен-ки	Итог. аттес. (Экза-мен)
1	ПМ.01. Применение комплексов средств автоматизации общего и специального назначения	384	258	68	110	74	126			6
2	ПМ.02. Эксплуатация инфокоммуникационного оборудования сетей и узлов (предприятий) связи	110	74	10	40	18	36			6
3	ПМ.03. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи	78	60	32	22		18			6
4	Итоговая аттестация (комплексный квалификационный экзамен	8	8							8
5	Итого:	580	400	110	172	92	180			26

в) Календарный учебный график

Учебные занятия (400 часов)	Практика (не предусмотрена)	Итоговая аттестация (Комплексный квалификационный экзамен – 8 часов)

Заместитель генерального директора
по научной работе И.А. Кулешов

Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.01. ПРИМЕНЕНИЕ КОМПЛЕКСОВ СРЕДСТВ АВТОМАТИЗАЦИИ ОБЩЕГО И СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ»

Санкт-Петербург
2023

Рабочая программа профессионального модуля является частью дополнительной профессиональной программы профессиональной переподготовки специалистов связи – администраторов инфокоммуникационных сетей.

1. Место профессионального модуля в структуре дополнительной профессиональной программы профессиональной переподготовки

Профессиональный модуль «Применение комплексов средств автоматизации общего и специального назначения» принадлежит к профессиональному циклу и является основой дополнительной профессиональной программы профессиональной переподготовки специалистов связи – администраторов инфокоммуникационных сетей.

Профессиональный модуль не требует изучения предшествующих дисциплин. Изучение учебного материала профессионального модуля базируется на знаниях специалистов не ниже уровня выпускников высших технических ВУЗов РФ (на базе высшего профессионального образования).

2. Цель и планируемые результаты обучения по профессиональному модулю

Целью профессионального модуля является приобретение новых (углубление) теоретических знаний и развитие практических умений, необходимых для профессиональной деятельности специалистов по применению электронно-вычислительной техники, комплексов средств автоматизации на узлах (предприятиях) связи общего и специального назначения, приобретения новых компетенций в рамках имеющейся квалификации.

Процесс изучения дисциплины направлен на формирование следующих компетенций:

способен обеспечивать эффективное использование эксплуатационных свойств и технических возможностей электронно-вычислительной техники, комплексов средств автоматизации в различных условиях обстановки;

способен применять технические, программные и информационные средства сетевых и информационных технологий в АСУ общего и специального назначения.

В результате освоения дисциплины специалист должен:

иметь представление:

о назначении и принципах построения глобальных и локальных вычислительных сетей;

об обеспечении безопасности персонала узла (предприятия) связи при эксплуатации КСА;

о концептуальных основах защиты информации в АСУ общего и специального назначения;

о перспективах развития информационных технологий и их применения в системах управления инфокоммуникационными сетями;

знать:

архитектуру, протоколы, базовые средства вычислительных сетей;

характеристики и возможности технических средств построения КСА;

возможности базовых средств новых информационных технологий;

особенности применения базовых сетевых технологий в системах телекоммуникаций;

основы построения информационных систем и проектирования баз данных;

основные протоколы, применяемые на инфокоммуникационных сетях общего и специального назначения;

возможности, тактико-технические характеристики и правила эксплуатации программно-технических средств узлов (предприятий) связи;

организационно-технические принципы построения инфокоммуникационных сетей общего и специального назначения;

содержание и организацию технической эксплуатации, ввода в эксплуатацию и обслуживания КСА общего и специального назначения;

состав и способы конфигурирования, эксплуатации и обслуживания программного обеспечения инфокоммуникационной сети;

содержание и организацию защиты информации в автоматизированных системах общего и специального назначения;

уметь:

применять технические и программные средства сетевых и информационных технологий в АСУ общего и специального назначения;

использовать системы управления базами данных для администрирования и актуализации информационных ресурсов;

применять средства конфигурирования КСА на базе локальных вычислительных сетей и персональных ЭВМ, обеспечивать инсталляцию, настройку и сопровождение программного обеспечения КСА;

выполнять ввод в эксплуатацию и обслуживание КСА;

использовать технические и программные средства современного цифрового телекоммуникационного оборудования в составе узла (предприятия) связи;

применять средства защиты информации в КСА общего и специального назначения;

обучать персонал узлов (предприятий) связи технически правильной эксплуатации инфокоммуникационного оборудования;

владеть:

навыками настройки, конфигурирования, тестирования, эксплуатации и технического обслуживания инфокоммуникационного оборудования узлов (предприятий) связи и его программного обеспечения.

3. Объем учебной дисциплины:

обязательной аудиторной учебной нагрузки обучающегося – 400 часов; самостоятельной работы обучающегося 180 часов.

4. Содержание и структура профессионального модуля

4.1. Распределение учебного времени по темам и видам учебных занятий

Наименование дисциплин, разделов и тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий						Время на самостоятельную работу	Экзамены, зачеты
			Лекции	Семинары	Практические занятия	Лабораторные работы	Групповые занятия	Курсовые раЬоты		
1	2	3	4	5	6	7	8	9	10	11
Раздел 1. Базовые средства построения вычислительных сетей										
Тема 1. Архитектура вычислительных сетей	15	10	8				2		5	
Тема 2. Построение локальных вычислительных сетей	30	20	4		6		10		10	
Тема 3. Протоколы вычислительных сетей	33	22	2		10		10		11	
Тема 4. Программное обеспечение ЛВС	33	22	4		8		10		11	
Раздел 2. Базовые средства новых информационных технологий										
Тема 5. Современные информационные технологии	42	28	6		14		8		14	
Тема 6. Технологии информационного обслуживания должностных лиц	45	30	6		18		6		15	
Тема 7. Технологии обработки данных	33	22	6		12		4		11	
Тема 8. Техническое и программное обеспечение систем обмена информацией и электронного документооборота	33	22	4		14		4		11	
Раздел 3. **Организация технической эксплуатации КСА**										
Тема 9. Система и мероприятия технической эксплуатации КСА	15	10	4				6		5	
Тема 10. Организация управления технической эксплуатацией и оперативно-технической службы на объектах размещения КСА	45	30	6		14		10		15	
Раздел 4. Защита информации в АСУ военного назначения										
Тема 11. Концептуальные основы защиты информации	6	4	4						2	
Тема 12. Защита информации от несанкционированного доступа в автоматизированную систему	15	10	4		6				5	
Тема 13. Защита информации от вредоносных программ и компьютерных атак	18	12	6		4		2		6	
Тема 14. Организации защиты информации в АС военного назначения	15	10	4		4		2		5	
Итоговый контроль	6	6								6
Всего по дисциплине:	**378**	**252**	**68**		**110**		**74**		**126**	**6**

4.2. Содержание разделов и тем

Раздел 1. Базовые средства построения вычислительных сетей

Тема 1. Архитектура вычислительных сетей

Введение. Цели, задачи дисциплины и роль подготовки специалистов по применению КСА на инфотелекоммуникационных системах и сетях.

Назначение, принципы построения, классификация и возможности вычислительных сетей (ВС). Логическая и физическая структуры ВС. Конфигурация глобальных вычислительных сетей и методы коммутации в них. Концепция системы автоматизации управления (САУ) и КСА общего и специального назначения.

Тема 2. Построение локальных вычислительных сетей

Концепция локальных вычислительных сетей (ЛВС). Протоколы, основные типы структур и базовые средства ЛВС. Характеристика и возможности технических средств построения КСА на базе ЛВС. Характеристика программных средств ЛВС. Основы проектирования ЛВС.

Тема 3. Протоколы вычислительных сетей

Вычислительные сети с коммутацией пакетов. Адресация в Intemet/Intranet. Основные услуги и протоколы Intemet/Intranet. Применение средств сетевых и информационных технологий в АСУ общего и специального назначения.

Тема 4. Программное обеспечение ЛВС

Назначение, состав и функциональные возможности базовых сетевых операционных систем. Применение средств конфигурирования КСА на базе ЛВС и персональных ЭВМ. Администрирование и работа с базовой сетевой операционной системой. Инсталляция, настройка и сопровождение программного обеспечения КСА.

Раздел 2. Базовые средства новых информационных технологий.

Тема 5. Современные информационные технологии

Технология электронного ведения документов. Возможности текстовых редакторов и табличных процессоров. Основы работы с текстовым редактором и табличным процессором. Разработка гипертекстовых документов. Обработка графической информации. Геоинформационные технологии. Построение систем мультимедиа.

Тема 6. Технологии информационного обслуживания должностных лиц узлов (предприятий) связи

Основы построения информационных систем. Основы проектирования баз данных. Современные системы управления баз данных, применение СУБД для администрирования и актуализации информационных ресурсов. Заведение и корректировка базы данных. Создание форм, формирование и выполнение запросов и отчетов. Разработка базы данных в интересах управления технической эксплуатацией КСА.

Тема 7. Технологии обработки данных

Концепция распределенной обработки данных. Технологии виртуализации и облачных вычислений. Организация удаленного доступа. Применение программных средств виртуализации.

Тема 8. Техническое и программное обеспечение систем обмена информацией и электронного документооборота

Техническое и программное обеспечение системы обмена информацией в электронном виде на узлах (предприятиях) связи. Построение системы электронного документооборота.

Раздел 3. Организация технической эксплуатации комплексов средств автоматизации

Тема 9. Система и мероприятия технической эксплуатации КСА

Содержание и организация технической эксплуатации КСА. Обеспечение безопасности персонала узлов (предприятий) связи при технической эксплуатации КСА. Ввод в эксплуатацию и обслуживание КСА общего и специального назначения.

Тема 10. Организация управления технической эксплуатацией и оперативно-технической службы на объектах размещения КСА

Система организационно-технологического управления КСА. Система планирования технической эксплуатации и ремонта КСА. Планирующие документы по технической эксплуатации КСА. Средства сетевого планирования мероприятий. Содержание и задачи ОТС на объектах размещения КСА. Разработка документов по ОТС для центра АСУ. Планирование подготовки и проведения технического обслуживания КСА.

Раздел 4. Защита информации в АСУ общего и специального назначения

Тема 11. Концептуальные основы защиты информации.

Концептуальные основы защиты информации в автоматизированных системах общего и специального назначения. Правовые основы защиты информации. Угрозы безопасности информации в автоматизированных системах общего и специального назначения. Методы и средства обеспечения безопасности информации в автоматизированных системах.

Тема 12. Защита информации от несанкционированного доступа в автоматизированных системах.

Концепция защиты от несанкционированного доступа к информации в автоматизированных системах. Модели, методы и средства защиты информации от несанкционированного доступа. Применение средств управления доступом, регистрации и учета, криптографических средств защиты информации, обеспечения целостности информации.

Тема 13. Защита информации от вредоносных программ и компьютерных атак.

Компьютерные вирусы и программные закладки. Защита от компьютерных вирусов и программных закладок. Настройка и применение средств защиты от вредоносных программ. Компьютерные атаки и способы защиты от них. Настройка и применение средств защиты от программных атак. Межсетевые экраны. Системы обнаружения атак.

Тема 14. Организация защиты информации в автоматизированных системах общего и специального назначения.

Содержание и организация защиты информации от несанкционированного доступа в автоматизированных системах общего и специального назначения. Разработка документов по защите информации. Применение средств защиты информации от несанкционированного доступа на объектах АСУ.

Перспективы развития информационных технологий и их применение на инфокоммуникационных сетях.

Формами текущего контроля за усвоением учебного материала являются **текущий опрос** слушателей на всех видах занятий, **оценка** выступлений и реферативных сообщений на групповых занятиях, выполнения заданий на групповых и практических занятиях.

Освоение профессионального модуля дополнительной профессиональной программы профессиональной переподготовки завершается промежуточной аттестацией в виде экзамена.

5. Методические рекомендации преподавателям

Во введении формулируются проблемы, возникающие при компьютеризации, проводимой в войсках, акцентируется внимание слушателей на роли подготовки специалистов по применению ЭВТ, дается характеристика учебной дисциплины.

В первом разделе рассматриваются базовые средства для построения вычислительных сетей.

Во втором разделе изучаются базовые средства информационных технологий по подготовке документов и обслуживанию должностных лиц.

В третьем разделе рассматриваются вопросы организации технической эксплуатации и обслуживания комплексов средств автоматизации.

В четвертом разделе изучаются вопросы защиты информации в системах и комплексах средств автоматизации общего и специального назначения. Рассматриваются методы защиты информации от несанкционированного доступа, компьютерных вирусов и средств специального программного воздействия.

В заключении слушателям дается представление о перспективах развития информационных технологий и их применения в системах управления связью, на узлах (предприятиях) связи.

Изучение дисциплины осуществляется путём чтения лекций, проведения групповых, практических занятий и самостоятельной работы обучающихся.

Теоретическая подготовка обучающихся включает чтение лекций, по наиболее важным и сложным вопросам.

Практическая подготовка обучающихся включает:

проведение по основным темам учебной программы групповых, практических занятий с целью получения практических навыков.

Уровень обученности «Знать» достигается проведением цикла занятий, включающим лекции.

Уровень обученности «Уметь» достигается проведением групповых и практических занятий.

Текущий контроль успеваемости обучающихся осуществляется на всех видах учебных занятий.

Обучение заканчивается итоговой аттестацией в виде экзамена, которая завершает освоение дополнительной образовательной программы профессиональной переподготовки специалистов связи – администраторов инфокоммуникационных сетей.

6. Методические указания обучающимся

Для успешного освоения профессионального модуля обучающиеся должны быть подготовлены в объёме программ высших технических ВУЗов РФ (на базе высшего профессионального образования).

Изучение профессионального модуля должно дать обучающимся понимание сущности, целей, задач и процессов построения и применения современных технических, программных и информационных средств электронно-вычислительной техники. Целевая направленность профессионального модуля связана с подготовкой специалистов, владеющих современными техническими и программными средствами электронного документооборота, администрирования (конфигурирования) инфокоммуникационных сетей.

Успешное изучение профессионального модуля предполагает эффективную самостоятельную работу обучаемых. Особое внимание данному виду подготовки следует уделить обучаемым, прибывшим с должностей не соответствующим профилю подготовки и не имеющих необходимого начального уровня подготовки.

7. Учебно-материальная база дисциплины и литература

Лекции проводятся в групповой аудитории, оснащенной мультимедийными средствами отображения информации и необходимым количеством посадочных мест.

Для проведения практических видов занятий и самостоятельной подготовки обучающиеся обеспечиваются аудиторией со средствами вычислительной техники, объединёнными в локальную вычислительную сеть, из расчета: одна персональная ЭВМ на одного-двух слушателей.

Реализация дополнительной профессиональной программы профессиональной переподготовки обеспечивается библиотечными и учебно-информационными фондами ПАО «Интелтех».

Дисциплина учебного плана дополнительной профессиональной программы профессиональной переподготовки обеспечивается учебно-методической литературой по всем видам учебных занятий и всему объёму самостоятельной работы слушателей, а также соответствующими лицензионными программными продуктами.

Обеспеченность учебно-методической литературой, соответствующей по содержанию изучаемому профессиональному модулю, – не менее одного экземпляра на двух слушателей.

Литература

№ п/п	Наименование и название литературы
	Основная
1.	Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.
2.	Саенко И.Б., Деньжонков К.А., Кий А.В., Чирушкин К.А. и др. Основы построения и администрирования операционной системы МСВС. Учебн. пособие/ Под ред. И.Б. Саенко. СПб.: ВАС, 2015. 156с.
3.	Анфилатов В.С., Авраменко В.С., Пантюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть 2. Основы построения и функционирования систем автоматизации управления войсками и связью: Учеб, пособие. СПб.: ВАС, 2015. 304с.
4.	Беззубов О.В., Ренсков А.А., Хилько В.О., Пантюхин О.И., Гудков М.А. Инженерная и компьютерная графика. Учебное пособие. – СПб.: ВАС, 2016. – 164с.
5.	Бударин Э.А., Дементьев В.Е. Обеспечение защиты информации в локальных вычислительных сетях. СПб.: ВАС, 2013. 228 с.
6.	Модели, методы и средства обнаружения распределенных компьютерных атак: учебное пособие / М.А. Еремеев, С.В. Новиков, В.А. Овчаров. – СПб.: ВКА им. А.Ф. Можайского, 2014. – 100 с.
	Дополнительная
7.	Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые информационные технологии в системах военного назначения. Учебник / Под редакцией И.Б. Саенко. СПб.: ВАС, 2010. 520 с.
8.	Новые информационные и сетевые технологии в системах управления военного назначения. Часть 1. Новые сетевые технологии в системах управления военного назначения. Учебник / Под ред. А.А. Одоевского. СПб.: ВАС, 2010. 500с.
9.	Авраменко В.С., Ильина О.Б., Морозов И. В. и др. Система обмена информацией в электронном виде Вооруженных сил Российской Федерации. Часть 1. Общие положения по построению системы обмена информации в электронном виде ВС РФ. Учебное пособие. – СПб.: ВАС, 2011. – 308 с.
10.	Авраменко В.С., Копчак Я.М., Бушуев С.Н., Саенко И.Б., Гузов М. В. Организация защиты информации в системах автоматизированного управления войсками и связью. Учебное пособие для вузов. Часть 1. – СПб.: ВАС, 2008. – 128 с.

8. Фонды оценочных средств и критерии оценки результатов обучения

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной тематическим планом с выставлением оценок в журнал.

8.1. Фонд оценочных средств

а) Теоретическая часть

1) Назначение и возможности вычислительных сетей в автоматизированных системах управления узлом (предприятием) связи.
2) Характеристики и возможности технических средств построения КСА.
3) Концепция локальных вычислительных сетей.
4) Архитектура и типы структур локальных вычислительных сетей.
5) Базовые протоколы локальных вычислительных сетей.
6) Технологии построения локальных вычислительных сетей.
7) Базовые средства локальных вычислительных сетей.
8) Назначение и классификация сетевых операционных систем.
9) Состав и функции сетевой операционной системы.
10) Возможности базовых средств новых информационных технологий.
11) Геоинформационные технологии и средства построения геоинформационных систем.
12) Основы построения информационных систем.
13) Основы проектирования баз данных.
14) Системы управления базами данных.
15) Модели данных информационных систем.
16) Построение и программное обеспечение системы обмена информацией в электронном виде на узлах (предприятиях) связи.
17) Назначение и структура службы доменных имен.
18) Системы электронного документооборота (СЭД). Назначение и состав СЭД.
19) Содержание и организация технической эксплуатации КСА общего и специального назначения.
20) Характеристика мероприятий ввода в эксплуатацию и обслуживания КСА общего и специального назначения.
21) Обеспечение безопасности персонала узлов (предприятий) связи при эксплуатации КСА.
22) Средства сетевого планирования мероприятий.
23) Концептуальных основы защиты информации в АСУ общего и специального назначения.
24) Методы и средства обеспечения безопасности информации в автоматизированных системах.

25) Концепция защиты от несанкционированного доступа к информации в автоматизированных системах общего и специального назначения.

26) Модели, методы и средства защиты от несанкционированного доступа (НСД).

27) Компьютерные вирусы и программные закладки.

28) Защита от компьютерных вирусов и программных закладок.

29) Программные атаки и способы защиты от них.

30) Содержание и организация защиты информации в АСУ общего и специального назначения.

31) Порядок разработки документов по защите информации от НСД.

б) Практическая часть

Практическое задание №1.

Разработка структуры информационно-расчетной системы на базе локальной вычислительной сети (ЛВС) узла (предприятия) связи. Исходные данные варианта выдаются экзаменатором.

Практическое задание №2.

Разработка таблиц адресования ПЭВМ в локальной вычислительной сети (ЛВС) на узле (предприятии) связи. Исходные данные варианта выдаются экзаменатором.

Практическое задание №3.

Разработка фрагмента базы данных в интересах должностных лиц узла (предприятия) связи и актуализация базы данных. Исходные данные варианта выдаются экзаменатором.

Практическое задание №4.

Настройка службы доменных имен (DNS) системы обмена информацией на сервере общего назначения. Исходные данные варианта выдаются экзаменатором.

Практическое задание №5.

Планирование проведения технического обслуживания ЛВС узла (предприятия) связи. Исходные данные варианта выдаются экзаменатором.

Практическое задание №6.

Планирование защиты информации от НСД в локальной вычислительной сети узла (предприятия) связи. Исходные данные варианта выдаются экзаменатором.

8.2 Критерии оценки результатов обучения при проведении текущего контроля и итоговой аттестации

Результаты текущего контроля определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Знания и умения обучающихся на экзамене определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

При осуществлении оценки уровня сформированности компетенций, умений и знаний, обучающихся и выставлении отметки целесообразно использовать аддитивный принцип (принцип «сложения»):

отметка «неудовлетворительно» выставляется обучающемуся, не показавшему освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, допустившему серьезные ошибки в выполнении предусмотренных программой заданий, не справившемуся с выполнением итоговой аттестационной работы;

отметку «удовлетворительно» заслуживает обучающийся, показавший частичное освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, сформированность не в полной мере новых компетенций и профессиональных умений для осуществления профессиональной деятельности, знакомый с литературой, публикациями по программе;

отметку «хорошо» заслуживает обучающийся, показавший освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой, изучивших литературу, рекомендованную программой, способный к самостоятельному пополнению и обновлению знаний в ходе дальнейшего обучения и профессиональной деятельности;

отметку «отлично» заслуживает обучающийся, показавший полное освоение планируемых результатов (знаний, умений, компетенций), всестороннее и глубокое изучение литературы, публикаций; умение выполнять задания с привнесением собственного видения проблемы, собственного варианта решения практической задачи, проявивший творческие способности в понимании и применении на практике содержания обучения.

Итоговая аттестация слушателей не может быть заменена оценкой уровня знаний на основе текущего контроля успеваемости и промежуточной аттестации слушателей.

По теоретической части билета с учетом ответов на дополнительные вопросы выставляется оценка по следующим критериям:

отлично – наличие глубоких исчерпывающих знаний в объеме пройденного профессионального модуля, правильные действия по применению полученных знаний при решении практических задач, грамотное и логически стройное изложение материала, знание содержания основной и дополнительно рекомендованной литературы;

хорошо – наличие твердых и достаточно полных знаний в объеме пройденного профессионального модуля при незначительных ошибках в освещении заданных вопросов, правильные действия по применению знаний при решении практических задач, четкое изложение материала;

удовлетворительно – наличие достаточных знаний в объеме пройденной дисциплины, изложение ответов без грубых ошибок, необходимость наводящих вопросов;

неудовлетворительно – наличие грубых ошибок в ответе, недопонимание сущности излагаемого вопроса, неумение применять знания при решении практических задач, неуверенность и неточности ответов на дополнительные вопросы. В случае отказа слушателя отвечать на теоретический вопрос билета по причине неподготовленности повторный

билет не предлагается и практическое задание не выдается. Немедленно выставляется итоговая оценка за зачёт – *неудовлетворительно.*

Критерии оценки по практической части:

отлично – задание выполнено правильно, слушатель умеет представить и интерпретировать результаты;

хорошо – при отработке практической части встретились незначительные затруднения, потребовавшие помощи со стороны преподавателя;

удовлетворительно – слушатель затруднялся с выбором и подготовкой к работе нужных программно-аппаратных средств или при выполнении задания возникли трудности, устраненные только после активной помощи преподавателя;

неудовлетворительно – слушатель не справился с заданием даже после многократной помощи преподавателя.

Итоговая оценка экзамена формируется в зависимости от оценок за теоретическую и практическую части ответа. При окончательном определении оценки за практическую и теоретическую части экзаменационного билета результирующая оценка не может быть выше оценки, полученной за практический вопрос.

Оценка за теоретическую часть	**Оценка за практическую часть**	**Итоговая оценка**
отлично	отлично	отлично
отлично	хорошо	хорошо
отлично	удовлетворительно	удовлетворительно
хорошо	отлично	отлично
хорошо	хорошо	хорошо
хорошо	удовлетворительно	удовлетворительно
удовлетворительно	отлично	хорошо
удовлетворительно	хорошо	хорошо
удовлетворительно	удовлетворительно	удовлетворительно
неудовлетворительно	отлично, хорошо, удовлетворительно	неудовлетворительно
отлично, хорошо, удовлетворительно	неудовлетворительно	неудовлетворительно

Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.02. ЭКСПЛУАТАЦИЯ ИНФОКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ СЕТЕЙ И УЗЛОВ (ПРЕДПРИЯТИЙ) СВЯЗИ»

Санкт-Петербург
2023

Рабочая программа профессионального модуля является частью дополнительной профессиональной программы повышения квалификации специалистов связи – администраторов инфокоммуникационных сетей (дополнительная к высшему профессиональному образованию).

1. Место профессионального модуля в структуре дополнительной профессиональной программы:

Профессиональный модуль «ПМ.02. Эксплуатация инфокоммуникационного оборудования сетей и узлов (предприятий) связи» является самостоятельной, не требует изучения предшествующих дисциплин и базируется на знаниях, умениях и навыках, полученных обучающимися в ходе повседневной деятельности.

2. Цель и планируемые результаты обучения по профессиональному модулю

Целью профессионального модуля является совершенствование уровня общепрофессиональной подготовки специалистов в области сетей связи и систем коммутации общего и специального назначения.

В результате освоения профессионального модуля специалист должен:

знать:

возможности, тактико-технические характеристики и правила эксплуатации программно-технических средств узлов (предприятий) связи;

организационно-технические принципы построения инфокоммуникационных сетей общего и специального назначения;

основные протоколы, применяемые на инфокоммуникационных сетях общего и специального назначения;

особенности применения базовых сетевых технологий в системах телекоммуникаций;

основы обеспечения безопасности информации на сети;

состав и способы конфигурирования, эксплуатации и обслуживания программного обеспечения инфокоммуникационной сети;

уметь:

готовить к работе и эксплуатировать на узлах связи изучаемые программно-технические средства связи, обеспечивать связь в различных режимах работы;

использовать технические и программные средства современного цифрового телекоммуникационного оборудования в составе узла (предприятия) связи;

обслуживать используемое оборудование и работать с технической документацией по данному оборудованию;

осуществлять технический контроль за функционированием оборудования;

эксплуатировать комплексы программных средств обработки и защиты информации инфокоммуникационной сети;

владеть:

навыками настройки, конфигурирования, тестирования, эксплуатации и технического обслуживания инфокоммуникационного оборудования узлов (предприятий) связи и его программного обеспечения.

3. Объем учебной дисциплины:

обязательной аудиторной учебной нагрузки обучающегося 72 часа; самостоятельной работы обучающегося 36 часов.

4. Структура и содержание учебной дисциплины

4.1 Распределение учебного времени по темам и видам учебных занятий:

Наименование дисциплин, разделов и тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий							Время на самостоятельную работу	Экзамены, зачеты
			Лекций:	Семинары	Практические занятия	Лабораторные работы	Групповые занятия	Контрольные работы	Инструктоско-методические занятия		
Тема 1. Базовые технологии формирования, передачи и коммутации данных в пакетных сетях.	18	12	10				2			6	
Тема 2. Конфигурирование, эксплуатация и обслуживание программного обеспечения инфокоммуникационной сети узла (предприятия) связи	24	16			16					8	
Тема 3. Конфигурирование, эксплуатация и обслуживание инфокоммуникационного оборудования узлов (предприятий) связи.	60	40			28		12			20	
Итоговый контроль	6	6									6
Всего по дисциплине:	108	74	10		44		14			36	6

4.2. Содержание разделов и тем

Тема 1. Базовые технологии формирования, передачи и коммутации данных в пакетных сетях

Облик телекоммуникационных сетей (ТКС) и систем на основе применения узлов связи объектов комплексного оснащения (УС ОКО). Организационно-техническая и логические структуры узла связи объекта комплексного оснащения. Принцип уровневой организации ТКС. Базовые протоколы и технологии мультисервисных сетей. Адресация в IP-сетях с решением практических задач. Маршрутизация в IP-сетях. Общие свойства и классификация протоколов маршрутизации. Пограничные маршрутизаторы узла, используемые на УС ОКО.

Тема 2. Конфигурирование, эксплуатация и обслуживание программного обеспечения инфокоммуникационной сети узла (предприятия) связи

Операционная система МСВС 3.0. Конфигурирование и обслуживание сервера доменных имён. Настройка служб единого времени (NTP) и гипертекстовой обработки данных («ГОД») и электронной почты. Управление комплексом защиты информации от несанкционированных действий (КСЗИ НСД).

Тема 3. Конфигурирование, эксплуатация и обслуживание инфокоммуникационного оборудования узлов (предприятий) связи

Основные и специальные требования по размещению изделий семейства КМ. Обеспечение безопасности шифрованной связи при эксплуатации изделий семейства КМ. Правила работы с ключевыми документами и изделием семейства КМ. Принципы функционирования и технические характеристики шлюзов VoIP. Порядок настройки и конфигурирования шлюза VoIP m.Gate-ITG. «Протей». Назначение, технические характеристики пограничного маршрутизатора узла (ПМУ) «Juniper SRX-240», настройка основных системных параметров и сетевых интерфейсов маршрутизатора «Juniper SRX-240». Назначение, состав и основные возможности УПАТС «МиниКом DX-500». Команды управления и конфигурирования УПАТС «МиниКом DX-500». Назначение, ТТХ и эксплуатация межсетевого экрана FW 16000. Назначение, ТТХ и эксплуатация криптомаршрутизатора КМ-07Ф. Набор связей в составе узла и сети в целом.

5. Методические рекомендации преподавателям

Базовые технологии формирования, передачи и коммутации данных в пакетных сетях излагать на лекциях, на которых развивать потребность к самостоятельной работе обучающихся по рекомендованной литературе. В ходе лекции организовать активную работу слушателей и постоянно поддерживать стремление к лучшему пониманию и усвоению материала.

На групповых занятиях изучать основы конфигурирования, эксплуатации и обслуживания инфокоммуникационного оборудования узлов (предприятий) связи.

На практических занятиях формировать умения в установке, настройке и техническом обслуживании комплекса программно-аппаратных средств инфокоммуникационного оборудования УС ОКО. Для проведения каждого практического занятия необходимо разрабатывать соответствующие задания, осуществлять строгий контроль деятельности обучающихся.

Для самостоятельной работы давать задания, направленные на закрепление знаний, полученных на других видах занятий, а также развитие навыков работы с литературой, технической документацией и инструкциями. В часы самостоятельной подготовки обучающихся преподавательскому составу проводить индивидуальные консультации, а перед проведением групповых и практических занятий – групповые консультации, где ставить задачи по углублению знаний и развитию профессиональных навыков.

Контроль успеваемости и качества подготовки слушателей по дисциплине проводить в форме текущего и рубежного контроля.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, своевременного вскрытия недостатков в подготовке обучающихся и принятия мер по совершенствованию методики преподавания учебной дисциплины, оказание обучающимся индивидуальной помощи и побуждения их к более глубокой самостоятельной работе над учебными материалами. Он проводится в ходе всех видов учебных занятий в форме, избранной преподавателем. Результаты текущего контроля отражаются в журнале учета учебных занятий.

После изучения каждой темы, слушатели проходят тестирование, оценка за которое является одной из составляющих при определении результатов рубежного контроля.

Рубежный контроль осуществлять для проверки качества усвоения учебного материала и стимулирования учебной работы обучающихся. Рубежный контроль проводить путем устного и письменного опросов, выполнения учебных заданий с выставлением оценок 100 % обучающихся.

Итоговую аттестацию проводить с целью определения степени достижения учебных целей по дисциплине в форме зачета с оценкой. В экзаменационный билет включать два вопроса – теоретический и практический.

К итоговой аттестации допускать обучающихся, прошедших все этапы рубежного контроля, и имеющие по ним положительные оценки.

Результаты итоговой аттестации обсудить на заседании учебно-методического совета в целях совершенствования методики обучения.

6. Методические указания обучающимся

Профессиональный модуль состоит из трех тем, объединённых обшей целевой установкой.

Обучение по данным темам осуществляется на основе системного подхода, что позволяет сформировать более гибкие знания и умения по их применению в ходе решения задач.

В первой теме изучаются базовые технологи формирования, передачи и коммутации данных в пакетных сетях.

Во второй теме изучается конфигурирование, эксплуатация и обслуживание программного обеспечения инфокоммуникационной сети узла (предприятия) связи.

В третьей теме изучается конфигурирование, эксплуатация и обслуживание инфокоммуникационного оборудования узлов (предприятий) связи.

Уровень «владеть» обучающиеся достигают на практических занятиях, при проведении которых рекомендуется применять технологии поэтапного формирования умственных действий и кейс-технологии.

На самостоятельной подготовке обучающиеся закрепляют полученные на иных видах занятий знания. Для полного усвоения материала, приобретения знаний и практических навыков подготовка обучающихся осуществляется с обязательным ведением конспектов и самостоятельным изучением учебно-методической литературы, рекомендованной и разработанной в Учебном центре.

Для повышения эффективности обучения предполагается использование разработанных преподавательским составом Учебного центра, автоматизированных обучающих систем.

7. Учебно-материальная база дисциплины и литература

Для осуществления образовательного процесса по дисциплине необходима учебно-материальная база со следующим типом оборудования:

компьютерный класс с учебно-лабораторным стендом, ПЭВМ (АРМ) и установленными на их базе программами для использования при проведении практических занятий и контрольных работ;

специализированные аудитории для проведения групповых и практических занятий при изучении инфокоммуникационного оборудования.

Литература

№ п/п	Наименование и название литературы
Основная	
1.	Инфокоммуникационные системы специального назначения. Учебн. пособ. / Под ред. С.М. Одоевского. - СПб.: ВАС, 2017. – 456 с.
2.	Олифер В.Г., Олифер Н.А., Компьютерные сети. Учебник. 5-е изд.- СПб. «Питер», 2016. – 992 с.
3.	Сетевое оборудование комплексов связи специального назначения. [Электронный учебник] - СПб.: ВАС. 2016 URL: httD://kaf22/vas/local/imaees/EOK/SOCSSN/start.htm.
Дополнительная	
1.	Саенко И.Б. Ершов А.В. Ефимов В.В. Базовые защищенные компьютерные информационные технологии (руководство пользователя). Учебное пособие. - СПб.: ВАС, 2007. – 340 с.
2.	Эксплуатационная документация оборудования цифровой телекоммуникационной сети узла (предприятия) связи.
3.	Эксплуатационная документация программного обеспечения цифровой телекоммуникационной сети узла (предприятия) связи.

8. Фонды оценочных средств и критерии оценки результатов обучения

8.1. Рубежный контроль

Задание на занятие № 10

Вид занятия: Групповое
Тема занятия: Настройка сетевых интерфейсов и фильтров межсетевого экрана FW 16000
Вид контроля: Текущий контроль
Форма контроля: Письменный опрос
Перечень вопросов (заданий):

1) Дать название и краткую характеристику уровней ЭМВОС.
2) Назовите и дайте краткую характеристику видам устройств, используемых на УС ОКО.
3) Сколько хостов содержится в классе С.
4) Какой адрес маршрутизатор использует, чтобы сравнить с таблицей маршрутизации.
5) Какой корректный диапазон хостов для IP-адреса сети 10.168.168.188 255.255.255.192

Задание на занятие № 15

Вид занятия: Групповое
Тема занятия: Назначение, состав и основные возможности УПАТС «МиниКом DX-500»
Вид контроля: Текущий контроль
Форма контроля: Устный опрос
Перечень вопросов (заданий):

1) Что представляет собой изделие МСЭ FW 16000.
2) Какой гриф имеет изделие КМ-07Ф введенное в эксплуатацию на сети связи.
3) Для чего предназначено изделие КМ-07Ф.
4) С каким количеством сетей изделие МСЭ FW 16000 позволяет обеспечить обмен информационными данными по внутренним сетевым интерфейсам.
5) Перечислите основные функции, выполняемые интерфейсами в изделии FW 16000.

Задание на занятие № 19

Вид занятия: Практическое
Тема занятия: Набор связей в составе узла и сети в целом
Вид контроля: Текущий контроль
Форма контроля: Устный опрос
Перечень вопросов (заданий):

1) Перечислите все номера портов для третьего потока Е1 в первом кластере 0-го DX.

2) Содержание таблицы 'Port' в DX-500.

3) Приведите вариант правильного ввода команды для отображения конфигурации портов.

4) Приведите вариант правильного ввода команды для записи конфигурации 6-го параметра 0-го порта 0-го DX в 0 кластере.

5) Приведите вариант правильного ввода команды для отображения конфигурации портов.

8.2. Итоговая аттестация

Форма проведения итоговой аттестации – экзамен.

Критерии оценки итоговой аттестации

Основным критерием оценки подготовленности обучающихся является единство освоенных уровней обученности.

При определении оценки принимается во внимание:

точность ответов на вопросы тестовых заданий;

уровень практических умений слушателя при выполнении практического задания.

Уровень подготовленности аттестуемых оценивается на «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Результаты тестирования слушателей определяются следующими критериями:

оценка **«отлично»** выставляется, если количество правильных ответов на вопросы теста превышает 80% от общего количества вопросов;

оценка **«хорошо»** выставляется, если количество правильных ответов на вопросы теста находится в пределах от 70% до 79% включительно от общего количества вопросов;

оценка **«удовлетворительно»** выставляется, если количество правильных ответов на вопросы теста находится в пределах от 60% до 69% включительно от общего количества вопросов;

оценка **«неудовлетворительно»** выставляется, если обучающийся не выполнил требований на оценку «удовлетворительно».

Общая оценка за теоретическую часть аттестационного испытания выставляется в соответствии с таблицей 1.

Результаты выполнения практической части итоговой аттестации оцениваются на «зачтено» и «не зачтено».

Оценка «зачтено» выставляется в том случае, если аттестуемый **выполнил** практическое задание в установленный срок. В противном случае выставляется оценка «не зачтено».

Таблица 1

Оценка теоретической подготовленности	Оценки по вопросам	
	1 тестовое задание	2 тестовое задание
отлично	5	5
	5	4
	4	5
хорошо	4	4
	3	4(5)
	4(5)	3
удовлетворительно	3	3
	2	4(5)
	4(5)	2
неудовлетворительно	2	2
	2	3
	3	2

Итоговая оценка каждому слушателю выставляется на основании частных оценок, полученных им за выполнение теоретической и практической частей экзамена в соответствии с критериями, представленными в таблице 2.

Таблица 2

Итоговая оценка	Оценки по вопросам	
	теоретическая часть	практическая часть
отлично	5	зачтено
хорошо	4	зачтено
удовлетворительно	3	зачтено
неудовлетворительно	3 (4, 5)	не зачтено
	2	зачтено

При подготовке к проведению экзамена учитывается служебная записка ведущего преподавателя с ходатайством перед начальником Учебного центра об освобождении от сдачи зачета обучающихся, показавших отличные знания по результатам текущего и рубежного контроля. Пересдача с целью повышения текущих оценок перед экзаменом не допускается.

Члены аттестационной комиссии несут личную ответственность за правильность и объективность выставленной оценки.

Обсуждение результатов аттестационного испытания в отношении каждого слушателя проводится на закрытом заседании аттестационной комиссии. Решение об оценке принимается простым большинством голосов. При равном числе голосов голос председателя комиссии является решающим.

Результаты итоговой аттестации оформляются секретарем комиссии экзаменационной ведомостью и объявляются слушателям председателем комиссии на подведении итогов.

Перечень тем, вопросов, теоретических заданий, выносимых на итоговую аттестацию:

Тест № 1

1) Какой класс IP-адресов по умолчанию имеет наибольшее количество хостов.
2) Как часто маршрутизаторы обмениваются служебными сообщениями BGP-update.
3) Какой командой скопировать с хоста TFTP конфигурационный файл на флеш маршрутизатора.
4) Какая команда используется для входа в режим глобальной конфигурации маршрутизатора.
5) Какой корректный диапазон хостов для IP-адреса сети 10.168.168.188 255.255.255.192.
6) Как в другом виде представить маску подсети 11111111.11111111.11111111.10000000.
7) Как в сокращенной записи представить маску подсети 255.255.255.240.
8) На какие подсети делится закрытый сегмент сети узла связи.
9) В какую подсеть сети закрытого сегмента входит шлюз VOIP.
10) Как в сокращенной записи представить маску подсети 255.255.255.128.
11) Какой допустимый диапазон адресов хостов отведен для адресов АРМ должностных лиц.
12) Какое корректное значение маски подсети для АРМ должностных лиц.
13) Какое корректное значение маски подсети для серверов общего назначения.
14) Диапазон адресов Class C.
15) Сколько хостов содержится в классе C.
16) Какие типы маршрутов могут быть в таблице маршрутизации.
17) Каковы цели протокола маршрутизации.
18) Какая информация отсутствует в обновлениях RIPvl.
19) Период обновления для RIP.
20) Какой механизм встроен в IP, чтобы преодолеть циклы маршрутизации.
21) Какой адрес маршрутизатор использует, чтобы сравнить с таблицей маршрутизации.
22) На каком уровне эталонной модели открытых систем работает маршрутизатор.
23) Какие метрики маршрутов используются в протоколах маршрутизации.

Тест № 2

КМ-07Ф

1) Что представляет собой изделие.
2) Какой гриф имеет изделие, введенное в эксплуатацию на сети связи.
3) Для чего предназначено изделие.
4) С каким количеством сетей изделие позволяет обеспечить обмен информационными данными по внутренним сетевым интерфейсам.
5) С каким количеством сетей изделие позволяет обеспечить обмен информационными данными по внешним сетевым интерфейсам.
6) Через какой интерфейс осуществляется подключение изделия к каналу связи, соединяющему изделие с сетями общего доступа, через который передается защищаемая изделием информация Пользователя.
7) Через какой интерфейс осуществляется подключение изделия к каналу связи, соединяющему изделие с локальными вычислительными сетями (ЛВС), в которых циркулирует информация Пользователя, содержащая сведения, составляющие государственную тайну.
8) Перечислите основные функции обеспечиваемые изделием.
9) Согласно какому протоколу обеспечивается шифрование исходящих и расшифрование входящих через *внешний* интерфейс изделия IP-потоков данных.
10) Какой тип соединения возникает при установлении информационного взаимодействия между каждой парой криптомаршрутизаторов, расположенных на территориально разнесенных узлах ЗСПД, через сеть общего доступа.

МСЭ

1) Что представляет собой изделие DioNIS Security Server.
2) Чем является изделие DioNIS Security Server.
3) Для чего предназначено устройство защиты «Сторож», входящее в состав изделий.
4) Для чего предназначена плата «Аппаратный ключ защиты» входящая в состав изделий.
5) Что является основным объектом настройки изделия.
6) Что представляют из себя интерфейсы в изделии.
7) Перечислите основные функции выполняемые интерфейсами в изделии.

Шлюз VoIP

1) Назовите основные функции шлюза VoIP.
2) По каким протоколам осуществляется управление шлюза VoIP.
3) Какой протокол обеспечивает телефонную связь на пакетной сети.
4) Что необходимо выполнить для повышения надежности работы ЛВС.
5) На каких сетях работает шлюз VoIP.
6) Для чего предназначено изделие «СиТи-1Р-М».

7) Назовите основные функции реализуемые изделием «СиТи-1Р-М».

8) Сколько интерфейсов шлюза Е1 может быть реализовано в изделии «СиТи-1Р-М».

9) В каком сегменте сети функционирует изделие «СиТи-1Р-М».

10) Что представляет собой изделие mGate.ITG компании Протей.

11) Назовите основные функции реализуемые изделием mGate.ITG компании Протей.

12) Укажите поддерживаемые протоколы сигнализации VoIP изделием mGate.ITG компании Протей.

13) Укажите поддерживаемые протоколы сигнализации ТфОП изделием mGate.ITG компании Протей.

14) Согласно каким рекомендациям осуществляется кодирование речи в пакетном режиме изделием mGate.ITG компании Протей.

15) В каком сегменте сети функционирует изделие mGate.ITG компании Протей.

16) Укажите скорость цифрового потока для одного тракта Е1 изделия mGate.ITG компании Протей.

DX-500

1) Какие возможные причины повреждения модулей DX-500 при загорании светодиодов +5V, -5V.

2) Какие возможные причины повреждения модулей DX-500 при загорании светодиода M51.

3) Какие возможные причины неисправности при загорании светодиодов Vin A.

4) Какие возможные причины неисправности при медленном мигании светодидов LOCAL на модулях DX-500.

5) Перечислите все номера портов для третьего потока Е1 в первом кластере 0-го DX.

6) Содержание таблицы 'Port' в DX-500.

7) Приведите вариант правильного ввода команды для отображения конфигурации портов.

8) Приведите вариант правильного ввода команды для записи конфигурации 6-го параметра 0-го порта 0-го DX в 0 кластере.

9) Приведите пример команды для отображения таблицы плана нумерации.

10) Какой уровень доступа оператора к терминальной программе управления DX-500 позволяет просматривать конфигурационные данные, не изменяя их.

11) Ваши действия если светодиод H.FLT на аналоговых кластерах DX-500N-ADK (DX-500M-ADK-CO) быстро мигает.

12) Содержание таблицы 'Portd' в DX-500.

13) Содержание таблицы ' Paddp ' в DX-500.

14) На каких модулях станции DX-500 установлены контроллеры портов RS-232.

15) Какие модули могут размещаться в кассете «МиниКом DX-500-Сг250-1».

16) Какое допустимое сопротивление шлейфа абонентского порта станции DX-500 (с телефонным аппаратом).

17) Какое допустимое сопротивление изоляции между проводами и между каждым проводом и землей DX-500 (с телефонным аппаратом).

18) Что включает в себя полугодовое техническое обслуживание на станции DX-500.

19) Для чего используется кнопка RESET на кластерах DX-500.

20) Приведите команду для анализа работоспособности ИКМ-каналов станции DX-500.

21) Перечислите основные функции, реализуемые DX-500.

22) Назначение абонентского кластера DX-500-ADK-CO.

23) Назначение модуля DX-500-16S.

24) Какой интерфейс реализует субмодуль DX-500-A02F.

25) Какой интерфейс реализует станция DX-500 со шлюзом VoIP.

Перечень тем, вопросов, практических заданий, выносимых на итоговую аттестацию:

Маршрутизатор Juniper SRX 240

1) Подключение к маршрутизатору. Вход в режим конфигурирования.
2) Создание локальной учетной записи пользователя.
3) Настройка последовательного интерфейса.
4) Настройка внешнего Ethemet-интерфейса.
5) Настройка внутреннего Ethemet-интерфейса.
6) Настройка межсетевой динамической маршрутизации.

КМ-07Ф

1) Согласно выданного задания произвести настройку внешних интерфейсов изделия.

2) Согласно выданного задания произвести настройку внутренних интерфейсов изделия.

3) Произвести проверку правильности настройки внешних и внутренних интерфейсов изделия, определить наличие ошибок и устранить их.

4) Согласно выданного задания сформировать туннель на направлении связи.

5) Проверить работоспособность сформированных туннелей и исправить обнаруженные ошибки.

МСЭ FW 16000.

22. Согласно выданного задания произвести настройку внешних интерфейсов МСЭ.

23. Согласно выданного задания произвести настройку внутренних интерфейсов МСЭ.

24. Произвести проверку правильности настройки внешних и внутренних интерфейсов, определить наличие ошибок и устранить их.

25. Согласно выданного задания создать и включить фильтр МСЭ.

DX-500

1) Присвоить абонентский списочный номер аналоговому порту станции DX-500.

2) Настроить цифровую соединительную линию E1 для работы со шлюзом VoIP.

3) Произвести тестирование системы по анализу статистических счетчиков, анализ работоспособности системы по показаниям счетчиков ошибок и очистку статистических счетчиков.

Шлюз VoIP «ПРОТЕЙ»

1) Согласно выданного задания настроить сетевые параметры на шлюзе VoIP Протэй.

2) Произвести настройку шлюза Протэй с предустановленной конфигурацией.

Вопросы для текущего, рубежного контроля и итоговой аттестации обучающихся изменяются в соответствии с изменениями нормативно-правовых актов, определяющих содержание учебной дисциплины.

Публичное акционерное общество
«Информационные телекоммуникационные технологии»
(ПАО «Интелтех»)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ»

Санкт-Петербург
2023

Рабочая программа профессионального модуля является частью дополнительной профессиональной программы повышения квалификации специалистов связи – администраторов инфокоммуникационных сетей (дополнительная к высшему профессиональному образованию).

1. Место профессионального модуля в структуре дополнительной профессиональной программы:

Профессиональный модуль «ПМ.03. Обеспечение информационной безопасности телекоммуникационных сетей и систем связи» является самостоятельной, не требует изучения предшествующих дисциплин и базируется на знаниях, умениях и навыках, полученных обучающимися в ходе повседневной деятельности.

2. Цель и планируемые результаты обучения по профессиональному модулю

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие компетенции и профессиональные компетенции.

Перечень общих компетенций:

Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

Планировать и реализовывать собственное профессиональное и личностное развитие.

Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.

Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

Использовать информационные технологии в профессиональной деятельности.

Пользоваться профессиональной документацией на государственном и иностранном языке.

Перечень профессиональных компетенций:

Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.

Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.

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

В результате освоения профессионального модуля специалист должен:

иметь практический опыт:

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

разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;

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

знать:

принципы построения информационно-коммуникационных сетей;

международные стандарты информационной безопасности для проводныхи беспроводных сетей;

нормативно-правовые и законодательные акты в области информационной безопасности;

акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;

технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

способы и методы обнаружения средств съёма информации в радиоканале;

классификацию угроз сетевой безопасности; характерные особенности сетевых атак;

возможные способы несанкционированного доступа к системам связи;

правила проведения возможных проверок согласно нормативных документов ФСТЭК;

этапы определения конфиденциальности документов объекта защиты;

назначение, классификацию и принципы работы специализированного оборудования;

методы и способы защиты информации беспроводных логических сетейот НСД посредством протоколов WEP, WPA и WPA 2;

методы и средства защиты информации в телекоммуникациях от вредоносных программ;

технологии применения программных продуктов;

возможные способы, места установки и настройки программных продуктов;

методы и способы защиты информации, передаваемой по кабельным направляющим системам;

конфигурации защищаемых сетей;

алгоритмы работы тестовых программ;

средства защиты различных операционных систем и среды передачи информации;

способы и методы шифрования (кодирование и декодирование) информации;

уметь:

классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

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

определять возможные сетевые атаки и способы несанкционированногодоступа в конвергентных системах связи;

осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;

выполнять тестирование систем с целью определения уровня защищенности;

определять оптимальные способы обеспечения информационной безопас-ности;

проводить выбор средств защиты в соответствии с выявленными угрозамив инфокоммуникационных сетях;

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

разрабатывать политику безопасности сетевых элементов и логических сетей;

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

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

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

защищать базы данных при помощи специализированных программных продуктов;

защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.

3. Объем профессионального модуля:

обязательной аудиторной учебной нагрузки обучающегося 60 часов; самостоятельной работы обучающегося 20 часов.

4. Структура и содержание учебной дисциплины

4.1 Распределение учебного времени по темам и видам учебных занятий:

№ пп	Наименование разделов и дисциплин (модулей)	Трудо-емкость	Всего ауд. часов	в том числе		Дистанци-онные занятия	Самост. работа, час	Форма контроля
				лекции	практич. занятия			
1	**Раздел 1**. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	32	26	16	10		6	Тести-рование
2	**Раздел 2.** Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	40	28	16	12		12	Тести-рование
3	Промежуточная аттестация (экзамен)	6	6					Экзамен
6	**Всего:**	78	60	32	22		18	

4.2. Содержание разделов и тем

Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

Тема 1.1. Основы безопасности информационных технологий

1) Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечениябезопасности информационных технологий.

2) Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.

3) Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности.

4) Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.

5) Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.

6) Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защитыинформации.

7) Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация иаутентификация пользователей.

8) Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности.

Тема 1.2. Обеспечениебезопасности информационных технологий.

1) Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ.

2) Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации

3) Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.

4) Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедур авторизации сотрудников.

5) Порядок изменения конфигурации программно- аппаратных средств. Обеспечение и контроль физической целостности и неизменности

конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.

6) Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.

7) Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.

8) Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.

9) Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации.

10) Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.

Тема 1.3. Средства защиты информации от несанкционированного доступа.

1) Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов.

2) Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к СЗИ.

3) Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации, например, DAL-LASLOCK

4) Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть»).

5) Назначение и особенности применения СЗИ НСД (например, «Страж NT»).

6) Назначение и специфика применения комплекса ЗИ (например, «Соболь»).

7) Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру от крытых ключей.

8) Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана.

9) Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности.

Тема 1.4. Обеспечение безопасности компьютерных систем и сетей

1) Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация.

2) Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.

3) Анализ содержимого почтового и WEB-трафика. HTTP-трафик.

4) Виртуальные частные сети. Решение на базе ОС Windows 2003. VPN на основе криптошлюза (например, «Континент-К»).

5) Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности.

6) Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.

Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи

Тема 2.1. Основы информационной безопасности.

1) Основные понятия информационной безопасности. Сущность и понятия защиты информации.

2) Значение информационной безопасности и ее место в системе национальной безопасности.

3) Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.

4) Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.

5) Состояние информационной безопасности РФ и основные задачи по ее обеспечению.

6) Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.

Тема 2.2. Организационно-правовые аспекты защиты информации.

1) Структура правовой защиты информации. Система документов в области защиты информации. Организационные основы защиты информации. Принципы организационной защиты информации.

2) Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации.

3) Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности.

4) Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.

Тема 2.3. Комплексная система защиты информации.

1) Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации.

2) Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.

3) Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.

4) Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.

5) Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.

Тема 2.4. Инженерно-техническая защита информации.

1) Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.

2) Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.

3) Технические каналы утечки информации. Общая структура канала утечки информации. Классификацияканалов утечки информации.

4) Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.

5) Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.

6) Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению.

7) Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальнойинформации. Защита информации в каналах связи.

8) Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания.

9) Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.

10) Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания. Контроль слаботочных цепей. Принципы контроля линий заземления.

11) Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.

12) Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.

Тема 2.5. Криптографическая защита информации.

1) Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.

2) Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования.

3) Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.

4) Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.

Тема 2.6. Аттестация и лицензирование объектов защиты.

1) Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.

2) Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.

3) Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.

5. Методические рекомендации преподавателям

Базовые технологии обеспечения информационной безопасности телекоммуникационных сетей и систем связи излагать на лекциях, на которых развивать потребность к самостоятельной работе обучающихся по рекомендованной литературе. В ходе лекции организовать активную работу слушателей и постоянно поддерживать стремление к лучшему пониманию и усвоению материала.

На практических занятиях формировать умения в установке, настройке и техническом обслуживании комплексов ТЗИ. Для проведения каждого практического занятия необходимо разрабатывать соответствующие задания, а на занятии осуществлять строгий контроль деятельности обучающихся.

Для самостоятельной работы давать задания, направленные на закрепление знаний, полученных на других видах занятий, а также развитие навыков работы с литературой, технической документацией и инструкциями.

В часы самостоятельной подготовки обучающихся преподавательскому составу проводить индивидуальные консультации, а перед проведением практических занятий – групповые консультации, где ставить задачи по углублению знаний и развитию профессиональных навыков.

Контроль успеваемости и качества подготовки слушателей по дисциплине проводить в форме текущего и рубежного контроля.

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, своевременного вскрытия недостатков в подготовке обучающихся и принятия мер по совершенствованию методики преподавания учебной дисциплины, оказания обучающимся индивидуальной помощи и побуждения их к более глубокой самостоятельной работе над учебными материалами. Он проводится в ходе всех видов учебных занятий в форме, избранной преподавателем. Результаты текущего контроля отражаются в журнале учета учебных занятий.

После изучения каждой темы, слушатели проходят тестирование, оценка за которое является одной из составляющих при определении результатов рубежного контроля.

Рубежный контроль осуществлять для проверки качества усвоения учебного материала и стимулирования учебной работы обучающихся. Рубежный контроль проводить путем устного и письменного опросов, выполнения учебных заданий с выставлением оценок 100 % обучающихся.

Итоговую аттестацию проводить с целью определения степени достижения учебных целей по дисциплине в форме зачета с оценкой. В экзаменационный билет включать два вопроса – теоретический и практический.

К итоговой аттестации допускать обучающихся, прошедших все этапы рубежного контроля, и имеющие по ним положительные оценки.

Результаты итоговой аттестации обсудить на заседании учебно-методического совета в целях совершенствования методики изучения дисциплины.

6. Методические указания обучающимся

Профессиональный модуль состоит из двух разделов, объединённых обшей целевой установкой.

Обучение по данным разделам осуществляется на основе системного подхода, что позволяет сформировать более гибкие знания и умения по их применению в ходе решения задач.

В первом разделе изучаются вопросы применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи.

Во втором разделе изучается вопросы применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи.

Уровень «уметь» обучающиеся достигают на практических занятиях, при проведении которых рекомендуется применять технологии поэтапного формирования умственных действий и кейс-технологии.

На самостоятельной подготовке обучающиеся закрепляют полученные на других видах занятий знания. В целях полного усвоения материала, приобретения знаний и практических навыков подготовка обучающихся должна осуществляться с обязательным ведением конспектов и самостоятельным изучением рекомендованной учебно-методической литературы, разработанной в Учебном центре.

Для повышения эффективности обучения предполагается использование разработанных преподавательским составом Учебного центра, автоматизированных обучающих систем.

7. Учебно-материальная база дисциплины и литература

Для осуществления образовательного процесса по дисциплине необходима учебно-материальная база со следующим типом оборудования:

компьютерный класс с учебно-лабораторным стендом, ПЭВМ (АРМ) и установленными на их базе программами для использования при проведении практических занятий и контрольных работ;

специализированные аудитории для проведения практических занятий при изучении средств ТЗИ.

Литература

7.2.1. Печатные издания

1. Партыка Т.Л., Попов И.И. Вычислительная техника: учеб. пособие. — М.: ФОРУМ: ИНФРА-М, 2017. — 445 с.

2. Арутюнов В.В. Защита информации: учебн.-метод. пособ. – Москва: Либерея-Бибинформ, 2008. – 55, с.

4. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность: учебн. пособ. – М.: Форум, 2015. – 528 с.

5. Мельников В.П., Клейменов С. А., Петраков А. М. Информационная безопасность: учебн. пособ. Под ред. С.А. Клейменова. – М.: Академия, 2013. – 331с.

6. Назаров А.В. Эксплуатация объектов сетевой инфраструктуры: учебник. – М.: Академия, 2014. – 368 с.

7.2.3. Дополнительные источники

1. Научно-технический журнал «Электросвязь»
2. Реферативный журнал «Вестник связи»
3. Научно-технический журнал «Сети и системы связи»
4. Реферативный журнал «Мобильные системы»
5. Научно-технический журнал «Цифровая обработка сигналов»

8 Итоговая аттестация

Форма проведения итоговой аттестации – экзамен.

Критерии оценки итоговой аттестации

Основным критерием оценки подготовленности обучающихся является единство освоенных уровней обученности.

При определении оценки принимается во внимание:

точность ответов на вопросы тестовых заданий;

уровень практических умений слушателя при выполнении практического задания.

Уровень подготовленности аттестуемых оценивается на «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Результаты тестирования слушателей определяются следующими критериями:

оценка **«отлично»** выставляется, если количество правильных ответов на вопросы теста превышает 80% от общего количества вопросов;

оценка **«хорошо»** выставляется, если количество правильных ответов на вопросы теста находится в пределах от 70% до 79% включительно от общего количества вопросов;

оценка **«удовлетворительно»** выставляется, если количество правильных ответов на вопросы теста находится в пределах от 60% до 69% включительно от общего количества вопросов;

оценка **«неудовлетворительно»** выставляется, если обучающийся не выполнил требований на оценку «удовлетворительно».

Общая оценка за теоретическую часть аттестационного испытания выставляется в соответствии с таблицей 1.

Результаты выполнения практической части итоговой аттестации оцениваются на «зачтено» и «не зачтено».

Оценка «зачтено» выставляется в том случае, если аттестуемый **выполнил** практическое задание в установленный срок. В противном случае выставляется оценка «не зачтено».

Таблица 1

Оценка теоретической подготовленности	Оценки по вопросам	
	1 тестовое задание	2 тестовое задание
отлично	5	5
	5	4
	4	5
хорошо	4	4
	3	4(5)
	4(5)	3
удовлетворительно	3	3
	2	4(5)
	4(5)	2
неудовлетворительно	2	2
	2	3
	3	2

Итоговая оценка каждому слушателю выставляется на основании частных оценок, полученных им за выполнение теоретической и практической частей экзамена в соответствии с критериями, представленными в таблице 2.

Таблица 2

Итоговая оценка	Оценки по вопросам	
	теоретическая часть	практическая часть
отлично	5	зачтено
хорошо	4	зачтено
удовлетворительно	3	зачтено
неудовлетворительно	3 (4, 5)	не зачтено
	2	зачтено

При подготовке к проведению экзамена учитывается служебная записка ведущего преподавателя с ходатайством перед начальником Учебного центра об освобождении от сдачи зачета обучающихся, показавших отличные знания по результатам текущего и рубежного контроля. Пересдача с целью повышения текущих оценок перед экзаменом не допускается.

Члены аттестационной комиссии несут личную ответственность за правильность и объективность выставленной оценки.

Обсуждение результатов аттестационного испытания в отношении каждого слушателя проводится на закрытом заседании аттестационной комиссии. Решение об оценке принимается простым большинством голосов. При равном числе голосов голос председателя комиссии является решающим.

Результаты итоговой аттестации оформляются секретарем комиссии экзаменационной ведомостью и объявляются слушателям председателем комиссии на подведении итогов.

Учебную программу разработали:

Ученый секретарь ПАО «Интелтех»
доктор технических наук, профессор П.А. Будко
Главный специалист НТЦ-1
доктор технических наук, профессор В.И. Курносов

Заместитель генерального директора
ПАО «Интелтех» по научной работе
доктор технических наук, доцент И.А. Кулешов
«____» _____ 2023 г.