

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Балашов Александр Александрович
Должность: Проректор по учебной работе
Дата подписания: 02.03.2026 16:24:20
Уникальный программный ключ:
159a23a86061c60c9ea58b6d4823a92e747fed78

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет
«Московский институт электронной техники»



УТВЕРЖДАЮ

Проректор по учебной работе

А.Г. Балашов

«26» 2026 г.

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА -
ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ
«СЕТЕВАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»**

Объем 256 часов

Москва 2026 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Цель программы – формирование у слушателей профессиональных компетенций, необходимых для выполнения нового вида профессиональной деятельности и приобретения новой квалификации.

1.2. Характеристика новой квалификации / нового вида профессиональной деятельности

Выпускникам программы присваивается квалификация «Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

Результатами подготовки слушателей по программе является получение компетенций, необходимых для выполнения нового вида профессиональной деятельности в области информационных технологий: администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы и выполнению трудовых функций в сфере Администрирования средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) (D/03.6).

Перечень и характеристика компетенций, подлежащих совершенствованию, и (или) перечень новых компетенций, формирующихся в результате освоения программы:

Область профессиональной деятельности: 06 Связь, информационные и коммуникационные технологии.

Наименование вида экономической деятельности: 62.09 Деятельность, связанная с использованием вычислительной техники и информационных технологий, прочая.

Укрупненная группа специальностей: 11.00.00 «Электроника, радиотехника и системы связи»

1.3. Требования к результатам освоения программы

Дополнительная профессиональная программа (программа профессиональной переподготовки) «Сетевая безопасность телекоммуникационных систем» разработана в соответствии со стандартами:

- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи (уровень бакалавриата), утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 930 (далее – ФГОС ВО);

- профессиональный стандарт «Специалист по администрированию сетевых устройств информационно-коммуникационных систем», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 5 октября 2015 г. N 686н.

Результаты освоения программы профессиональной переподготовки представлены в таблице 1.

Таблица 1 - Результаты освоения программы профессиональной переподготовки

Код и формулировка профессиональной /профессионально-специализированной компетенции	Трудовая функция в соответствии с профессиональным стандартом		Индикаторы достижения компетенций
	Наименование	Код	
ПК -1 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях	Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	D/03.6	Знания: программно-аппаратные средства и методы защиты информации в компьютерных сетях. Умения: выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях. Опыт деятельности: настройки программных и

Код и формулировка профессиональной /профессионально-специализированной компетенции	Трудовая функция в соответствии с профессиональным стандартом		Индикаторы достижения компетенций
	Наименование	Код	
			аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации.
ПК-2 Настраивает сетевое оборудование и средства межсетевого экранирования	Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	D/03.6	Знания: принципы работы сетевого оборудования; порядок реализации методов и средств межсетевого экранирования; принципы работы и правила эксплуатации применяемых программно-аппаратных средств защиты информации. Умения: настраивать сетевое оборудование и средств межсетевого экранирования; настраивать правила фильтрации пакетов в компьютерных сетях; конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях. Опыт деятельности: настройки сетевого оборудования и средств межсетевого экранирования; управления средствами межсетевого экранирования в компьютерных сетях.
ПК-3 Обеспечивает анализ сетевого трафика	Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	D/03.6	Знания: состав типовых конфигураций программно-аппаратных средств защиты информации и режимов их функционирования в компьютерных сетях; методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации. Умения: проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях; производить анализ эффективности программно-аппаратных средств защиты

Код и формулировка профессиональной /профессионально-специализированной компетенции	Трудовая функция в соответствии с профессиональным стандартом		Индикаторы достижения компетенций
	Наименование	Код	
			информации в компьютерных сетях; оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; настраивать средства анализа сетевого трафика. Опыт деятельности: формирования шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях; управления функционированием программно-аппаратных средств защиты информации в компьютерных сетях; контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях, настройки средств анализа сетевого трафика.
ПК-4Участвует в проектировании и развитии стратегии сетевой безопасности	Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов)	D/03.6	Знания: принципы функционирования сетевых протоколов, включающих криптографические алгоритмы; виды политик управления доступом и информационными потоками в компьютерных сетях; источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры; организационные меры по

Код и формулировка профессиональной /профессионально-специализированной компетенции	Трудовая функция в соответствии с профессиональным стандартом		Индикаторы достижения компетенций
	Наименование	Код	
			защите информации. Умения: оценивать угрозы безопасности информации в компьютерных сетях; обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях; анализировать схемы информационного взаимодействия; разрабатывать решения по информационной безопасности объектов сетевой инфраструктуры. Опыт деятельности: определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; анализа схемы информационного взаимодействия; разработки решения по информационной безопасности объектов сетевой инфраструктуры.

1.4. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

К обучению по программе допускаются лица, имеющие среднее профессиональное или высшее образование или получающие среднее профессиональное или высшее образование (при наличии соответствующей справки с указанием года окончания).

1.5. Трудоемкость обучения

Нормативная трудоемкость обучения по данной программе – 256 часов, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

1.6. Форма обучения

Форма обучения: очно-заочная, с использованием электронного обучения и дистанционных образовательных технологий.

1.7. Режим занятий

Обучение осуществляется без отрыва от работы. Учебная нагрузка устанавливается не более 12 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя. Продолжительность одного академического часа занятий — 40 минут.

2. СОДЕРЖАНИЕ ПРОГРАММЫ
2.1. Учебный план программы

№ п/п	Наименование учебных дисциплин / модулей	Всего, о, час	В том числе										Форма аттестаци и (час.)
			аудиторных					самостоятельная работа					
			лекции			практические / лабораторные занятия		очно- заочн ая	очно- заочн ая	очно- заочн ая	очно- заочн ая	очно- заочн ая	
			очно- заочн ая	заочн ая	очно- заочн ая								
1.	Элементы телекоммуникационных сетей	16	8					-			6		Зачет (2)
2.	Основы системного и сетевого администрирования	32	4					12			14		Зачет (2)
3.	Инфокоммуникационные системы и сети	32	16					8			6		Зачет (2)
4.	Безопасность телекоммуникационных систем и сетей	72	32					16			22		Зачет (2)
5.	Сетевые операционные системы и службы	16	4					8			2		Зачет (2)
6.	Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности	66	4					32			28		Зачет (2)
7.	Квантовые технологии обеспечения безопасности сетей	16	8					4			2		Зачет (2)
8.	Итоговая аттестация (демонстрационный экзамен)	6											
9.	Всего	256	76					80			66		14

2.2. Календарный учебный график

№ п п	Наименование раздела(модуля)	Учебные недели																																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37			
1	Элементы телекоммуникационных сетей	А	А	А	А	ПА																																			
2	Основы системного и сетевого администрирования					А	А	ПА																																	
3	Инфокоммуникационные системы и сети							А	А	А	А	А	А	А	ПА																										
4.	Безопасность телекоммуникационных систем и сетей															А	А	А	А	А	А	А	ПА																		
5	Сетевые операционные системы и службы																							А	А	А	ПА														
6	Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности																											А	А	А	А	А	А	А	А	ПА					
7	Квантовые технологии обеспечения безопасности сетей																																				А	А	ПА		
8	Итоговая аттестация																																								ИА

Условные обозначения:

А – аудиторное занятие (лекция, практическое занятие, самостоятельная работа); ПА – промежуточная аттестация; ИА - итоговая аттестация

3. РАБОЧИЕ ПРОГРАММЫ УЧЕБНЫХ ДИСЦИПЛИН (МОДУЛЕЙ), ПРАКТИК/ СТАЖИРОВОК

Рабочая программа содержит перечень разделов и тем, а также рассматриваемых в них вопросов с учетом их трудоемкости.

№ п/п	Наименование и краткое содержание раздела(модуля)	Объем, часов
1.	Элементы телекоммуникационных сетей: Коммутаторы, концентраторы, мосты, маршрутизаторы, модемы, межсетевые экраны, повторители, серверы и оконечное оборудование. Программное и аппаратное обеспечение сетей, топологии сетей.	16
2.	Основы системного и сетевого администрирования: Адресация в сетях связи, сетевые соединения, варианты построения топологий сетей связи, технология Ethernet, стандарты беспроводных сетей связи, сегментация локальных сетей, маршрутизация в IP сетях, конфигурирование локальной сети на базе коммутаторов, конфигурирование протоколов маршрутизации, конфигурирование технологии трансляции сетевых адресов	32
3.	Инфокоммуникационные системы и сети: в модуле даётся информации о принципах построения сетей связи, стандартизации сетевых технологий, коммутация каналов, коммутация пакетов, сетевых технологиях различных уровней OSI, конфигурировании локальных сетей, протоколов на сетевых устройствах, модель угроз, TCP/IP, сети WAN, LAN, PAN.	32
4.	Безопасность телекоммуникационных систем и сетей: постановка проблемы защиты информации в телекоммуникационных системах и устройствах, требования по защите информации к телекоммуникационным системам и устройствам, архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем, методы защиты информации в телекоммуникационных системах, защита от несанкционированного доступа и модели безопасности компьютерных систем, защищенные протоколы стека TCP/IP, исследование защищенности сетевых протоколов с использованием средств анализа сетевого трафика, доверенная загрузка вычислительных средств, разработка решений по защите объектов сетевой инфраструктуры	72
5.	Сетевые операционные системы и службы: Сетевые операционные системы, сетевая файловая система, обеспечение сетевого взаимодействия ОС, технологии и службы аутентификации, конфигурация службы контроля доступа, конфигурация технологии сетевого шлюза, настройка межсетевого экрана, конфигурация технологий виртуальных сетей связи	16
6.	Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности: Виртуальные локальные сети, качество обслуживания, Многоадресная рассылка. ограничение доступа к сети, управление коммутаторами, методы приоритизации трафика, методы управления доступом к инфокоммуникационным системам, удаленный доступ до сетевых устройств и сетей, аутентификация и ролевое разделение доступа, функции защиты программных и аппаратных компонентов устройств коммутаторов, управление сетевыми устройствами, анализ трафика, агрегирование каналов. настройка списков контроля доступа, настройка сетевого оборудования и средств межсетевого экранирования, настройка средств анализа сетевого трафика,	66
7.	Квантовые технологии обеспечения безопасности сетей: Квантовая механика для квантовой связи, основы оптики, протоколы квантовой связи, квантовое распределение ключей, основы квантовых повторителей, квантовая запутанность, квантовый интернет, квантовая защита сетей	16
9.	Промежуточная аттестация	14
	Итоговая аттестация	6

3.1. Учебно-методическое и информационное обеспечение учебных дисциплин

Для теоретической подготовки используются учебная литература и комплект теоретических материалов, в виде электронных презентаций к лекциям, содержащие основные определения, математический аппарат и иллюстративный материал.

Для подготовки к лабораторным работам используется лабораторный практикум, содержащий описание методов и подходов к выполнению лабораторных заданий.

Перечень учебной литературы:

1) Орешкин В.И. Основы цифровой радиосвязи [Текст]: Учеб. пособие / В.И. Орешкин, Ж.В. Чиркунова; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М. : МИЭТ, 2014. - 120 с.

2) Катунин Г.П., Мамчев Г.В., Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети [Электронный ресурс] : В 3-х т.: Учеб. Пособие.

3) Т. 2 : Радиосвязь, радиовещание, телевидение / Г. П. Катунин [и др.] ; Под ред. В.П. Шувалова. – 3-е изд., стер. – М. : Горячая линия-Телеком, 2014. – 672 с.

4) Берлин А.Н. Телекоммуникационные сети и устройства / А.Н. Берлин. - 2-е изд. - М.: ИНТУИТ, 2016. - 395 с. - URL: <https://e.lanbook.com/book/100525> (дата обращения: 28.04.2023). - ISBN 978-5-94774-896-3

5) Галатенко В.А. Основы информационной безопасности : Учеб. пособие. - 2-е изд. - М. : ИНТУИТ, 2016. - 266 с. - URL: <https://e.lanbook.com/book/100295> (дата обращения: 28.04.2023). - ISBN 978-5-94774-821-5

6) Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : Учеб. пособие / П.Н. Девянин. - М. : Горячая линия-Телеком, 2012. - 320 с. - URL: <https://e.lanbook.com/book/5150> (дата обращения: 28.04.2023). - ISBN 978-5-9912-0147-6.

7) Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: Учеб. пособие / Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - [2-е изд., стер.]. - М. : Горячая линия-Телеком, 2012. - 550 с. - ISBN 978-5-9912-0257-2:1306-80.

8) Иверсен В.Б. Разработка телетрафика и планирование сетей / В.Б. Иверсен. - 2-е изд. - М.: ИНТУИТ.РУ, 2016. - 616 с. - URL: <https://e.lanbook.com/book/100473> (дата обращения: 02.05.2023)

9) Технологии разработки и создания компьютерных сетей на базе аппаратуры D-LINK: Учеб. пособие / В.В. Баринов [и др.]. - М.: Горячая линия-Телеком, 2013. - 216 с. - URL: <https://e.lanbook.com/book/11826> (дата обращения: 02.05.2023). - ISBN 978-5-9912-0287-9

10) Телекоммуникационные системы и сети: В 3-х т.: Учеб. пособие. Т. 3 : Мультисервисные сети / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев; Под ред. В.П. Шувалова. - 2-е изд., стер. - М. : Горячая линия-Телеком, 2015. - 592 с. - URL: <https://e.lanbook.com/book/64092> (дата обращения: 02.05.2023). - ISBN 978-5-9912-0484-2.

11) Беленькая М.Н. Администрирование в информационных системах: Учеб. пособие / М.Н. Беленькая, С.Т. Малиновский, Н.В. Яковенко. - М. : Горячая линия-Телеком, 2011. - 400 с. - URL: <https://e.lanbook.com/book/5117> (дата обращения: 02.05.2023). - ISBN 978-5-9912-0164-3

Информационные ресурсы:

1) ГОСТ Р 51898 – 2002 Аспекты безопасности. Правила включения в стандарты = Safety aspects. Guidelines for their inclusion in standards: Национальный стандарт РФ : Введ. 01.01.2003. - М.: Стандартинформ, 2018. - URL: <https://docs.cntd.ru/document/1200030314> (дата обращения: 02.05.2023).

2) Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий / Гостехкомиссия России. - URL: <https://docs.cntd.ru/document/456058353?marker=2CBO408§ion=text> (дата обращения: 02.05.2023). - Режим доступа: по заказу демонстрации.

3) ГОСТ Р 51897-2011 Менеджмент риска. Термины и определения: Национальный стандарт РФ : Введ. 01.12.2012. - М.: Стандартинформ, 2019. - URL: <https://docs.cntd.ru/document/1200088035> (дата обращения: 02.05.2023).

4) ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности: Национальный стандарт РФ :Введ. 01.12.2011. - М.: Стандартинформ, 2011. - URL: <https://docs.cntd.ru/document/1200084141> (дата обращения: 02.05.2023).

5) Методика определения актуальных угроз безопасности персональных данных при их обработке и информационных системах персональных данных: Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г. – URL: <https://docs.cntd.ru/document/902266674> (дата обращения: 02.05.2023).

6) ГОСТ Р 50922-2006 Защита информации. Основные термины и определения: Национальный стандарт РФ :Введ. 01.02.2008. - М.: Стандартинформ, 2008. - URL: <https://docs.cntd.ru/document/1200058320> (дата обращения: 02.05.2023).

7) Р 50.1.056-2005 Техническая защита информации. Основные термины и определения: Рекомендации :Введ. 01.06.2006. - М.: Стандартинформ, 2006. - URL: <https://docs.cntd.ru/document/1200044768> (дата обращения: 02.05.2023). - Режим доступа: по заказу демонстрации.

8) ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель: Государственный стандарт РФ :Введ. 01.01.2000. - М.: Стандартинформ, 2006. - URL: <https://docs.cntd.ru/document/1200028699> (дата обращения: 02.05.2023).

9) ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации: Государственный стандарт РФ :Введ. 01.01.2000. - М.: Стандартинформ, 2006. - URL: <https://docs.cntd.ru/document/1200007766> (дата обращения: 02.05.2023).

10) ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: <https://docs.cntd.ru/document/1200161706> (дата обращения: 02.05.2023).

11) ГОСТ 34.11-2018. Информационная технология. Криптографическая защита информации. Функция хеширования: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: <https://docs.cntd.ru/document/1200161707> (дата обращения: 02.05.2023).

12) ГОСТ 34.12-2018. Информационная технология. Криптографическая защита информации. Блочные шифры: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: <https://docs.cntd.ru/document/12001617078> (дата обращения: 02.05.2023).

13) ГОСТ 34.13-2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров: Межгосударственный стандарт :Введ. 01.06.2019. - М.: Стандартинформ, 2020. - URL: <https://docs.cntd.ru/document/12001617079> (дата обращения: 02.05.2023).

14) Р 1323565.1.030-2018 Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3): Рекомендации по стандартизации: Введ. 01.06.2020. - М.: Стандартинформ, 2020. - URL: <https://docs.cntd.ru/document/573338314> (дата обращения: 02.05.2023). - Режим доступа: по заказу демонстрации.

3.2. Материально-техническое обеспечение учебных дисциплин

Компьютерная техника с возможностью подключения к сети «Интернет» и установленным программным обеспечением: Операционная система Microsoft Windows от 7 версии и выше, LibreOffice, браузер (Яндекс и пр.)

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятия	Наименование оборудования, программного обеспечения
Учебная аудитория	Лекции	Мультимедиа-проектор Экран, Доска аудиторная, ПЭВМ
Компьютерный класс	Семинары (практические занятия)	Cisco packet tracer, Cisco Software Development Kit (SDK), Huawei EnSP, Python, C-Teppa СиЭсПи, Snort, Zabbix, Suricata, Vipnet IDS, Wireshark, NetFlow, Linux, Коммутатор Arctika 4804ig. Коммутатор Cisco Catalyst 2960 24порта. Коммутатор Cisco WS-C3650-24TS-E Cisco Catalyst 365024 Port Data 4x1G Uplink IP. Коммутатор PIC8. Коммутатор COMPEX SAS2224, SN:96857744. Комплекс оборудования Cisco Wireless: Cisco AIR-AP1231G-E-K9. Маршрутизатор ROUTER Cisco 1721. Маршрутизатор D-Link DES-110016. Роутер беспроводной ASUS RT-N16
Помещение для самостоятельной работы обучающихся	Самостоятельная работа	Open Office, Acrobat reader DC Cisco packet tracer, Cisco Software Development Kit (SDK), Huawei EnSP, Python, C-Teppa СиЭсПи, Snort, Zabbix, Suricata, Vipnet IDS, Wireshark, NetFlow, Linux

3.3. Система контроля и оценивания

Оценка качества освоения дисциплины включает промежуточную и итоговую аттестацию обучающихся.

Промежуточный контроль знаний проводится преподавателем на основе оценивания результатов лабораторных работ и самостоятельной работы обучающихся.

Итоговая аттестация по дисциплине проводится в форме тестирования, расположенного на СДО iSpring по адресу <https://edu.miet.ru>. Для получения зачета по дисциплине необходимо верно ответить не менее, чем на 70% вопросов итогового тестирования.

Пример типовых тестовых заданий:

№ п/п	Дисциплина	Вопрос	Варианты ответа
1	Элементы телекоммуникационных сетей	Устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа «витая пара» называется?	а. сетевыми коммутаторами б. сетевым адаптером в. концентратором г. сетевым мостом
2		Аппаратным маршрутизатором или программным обеспечением для сопряжения компьютерных сетей, использующих разные протоколы, называется...	а. сетевым шлюзом б. концентратором в. сетевым адаптером г. сетевым мостом
3	Основы системного и сетевого администрирования	Какой тип интерфейса не имеет физического порта, связанного с ним?	а. Консоль б. Ethernet в. Последовательный порт г. Виртуальный интерфейс коммутатора (SVI)

4		Одноранговыми называются сети	а. соединенные через сервер б. соединенные одним кабелем в. в которых устройства равноправны г. в которых используется коммутатором
5	Инфокоммуникационные системы и сети	Какое утверждение о пропускной способности канала связи доказывается во второй теореме Шеннона?	а. Невозможность передачи неискаженной информации по ненадежным каналам б. Вероятность передачи неискаженной информации по каналу связи не зависит от пропускной способности данного канала связи и является постоянной величиной в. Невозможность искажения информации для данного канала связи при максимально возможной скорости передачи информации г. Отношение пропускной способности канала связи к скорости неискаженной передачи символов алфавита передаваемого сообщения должно быть больше или равно энтропии передачи одного символа
6		Укажите тенденции развития телекоммуникационных систем и сетей, предусматривающие совершенствование связи по сетевым и техническим (или технологическим) направлениям:	а. глобализация б. мультисервисность в. персонализация г. интеграция
7	Безопасность телекоммуникационных систем и сетей	Угроза компьютерной сети – это ...	а. вероятное событие б. детерминированное (всегда определенное) событие в. событие, происходящее периодически г. событие, инициируемое руководителем подразделения

8		Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...	а. несанкционированного управления удаленным компьютером б. внедрения агрессивного программного кода в рамках активных объектов Web-страниц в. перехвата или подмены данных на путях транспортировки г. вмешательства в личную жизнь пользователя
9	Сетевые операционные системы и службы	Совокупность программ, которые предназначены для управления ресурсами компьютера и вычислительными процессами, а также для организации взаимодействия пользователя с аппаратурой, называется	а. операционной системой б. файловой системой в. оболочкой г. утилитами
10		Операционная система выполняет функцию	а. обеспечения организации и хранения файлов б. подключения устройств ввода/вывода в. организации обмена данными между компьютером и различными периферийными устройствами г. организации диалога с пользователем, управления аппаратурой и ресурсами компьютера
11	Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности	Наиболее эффективное средство для защиты от сетевых атак	а. использование сетевых экранов или «firewall б. посещение только «надежных» Интернет-узлов в. использование антивирусных программ г. использование системы обнаружения вторжений
12		Узел А имеет IPv4-адрес и маску подсети 10.5.4.100 255.255.255.0. Какой из следующих адресов IPv4 будет находиться в той же сети, что и Host-A?	а. 10.5.4.1 б. 10.5.0.1 в. 10.5.4.99 г. 10.0.0.98 д. 10.5.100.4
13	Квантовые технологии обеспечения безопасности	Какая технологическая особенность лазерного излучения дает	а. Протяженность линий передачи

	сетей	теоретическую возможность проведения успешных PNS-атак?	б. Протокол с измененной конфигурацией состояний в. Использование многофотонных состояний г. Собственные шумы системы
14		Какие значения может принимать мера схожести максимально смешанных квантовых состояний?	а. 0 б.1 в. 1/3 г.1/4 д.1/32

Примеры практических заданий:

№ п/п	Дисциплина	Задание
1	Элементы телекоммуникационных сетей	Провести классификацию выданного оборудования (выдается комплект из не менее 5 различного оборудования).
2	Основы системного и сетевого администрирования	Для представленной сети для каждой подсети подобрать наиболее подходящий IP-адрес и префикс так, чтобы все требования к адресации были удовлетворены
3	Инфокоммуникационные системы и сети	В сетевом симуляторе произвести конфигурацию технологии контроля доступа с использованием одного устройства типа коммутатор и четырех оконечных устройств (далее ПК1- ПК4). Настроить списки контроля доступа для организации передачи информационных сообщений от устройств ПК1-ПК3 на устройство ПК4, запретить передачу информационных сообщений с устройств ПК3 и ПК3 на устройство ПК2.
4	Безопасность телекоммуникационных систем и сетей	Между двумя пользователями, использующими сеть Интернет необходимо организовать защищенный VoIP канал. Определить модели угроз и произвести настройку оборудования, позволяющего организовать указанный канал.
5	Сетевые операционные системы и службы	Используя ОС Windows подготовить автоматическое создание метрик и обеспечить наполнения найденных метрик данными для списка сервиса времени с столбцами, отображающими статистику работы сервиса: скорость отработки запросов и количество запросов.
6	Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности	Проанализировать настройки коммутатора в участке цепи. Для порта 1 выполнить следующие действия: 1. определить следующие параметры: максимальное количество MAC-адресов разрешенное на порту коммутатора, включенный режим реагирования на нарушения безопасности. 2. Установить следующие параметры: количество MAC-адресов разрешенное на порту коммутатора равным 2, режим реагирования на нарушения безопасности установить в положение «Shutdown». 3. Провести контроль выполнения настроек, используя команду show port-security interface
7	Квантовые технологии обеспечения безопасности сетей	Подобрать оборудование, протоколы и методы обеспечения квантовой безопасности системы видеоконференцсвязи между не менее 10 участников, находящихся на расстоянии не более 100 км друг от друга.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Описание учебно-методического и материально-технического обеспечения программы приведено в рабочих программах учебных дисциплин (модулей), практик/ стажировок.

5. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

5.1. Фонды оценочных средств для итоговой аттестации

5.1.1. Практические задания

Итоговая аттестация проводится в форме демонстрационного экзамена в формате комплексного практического задания (кейса) или хакатона и презентационной защиты.

Демонстрационный экзамен моделирует выполнение практического задания в условиях, приближенных к профессиональной деятельности. Участники работают индивидуально или в командах (3–5 человек). Результатом является готовый программный продукт/прототип. Для защиты практического задания слушателю необходимо продемонстрировать комиссии работу разработанного интеллектуального агента, оформленную отчетную документацию.

Примеры заданий:

- 1) Проведение конфигурации маршрутизатора на базе ОС GNU Linux, создав квантово-устойчивого канала передачи данных, используя удаленный доступ.
- 2) Создать шаблон конфигурации OSPF со следующими переменными параметрами: номер процесса, интерфейсы, на которых нужно включить OSPF.
- 3) Настроить имеющийся комплект сетевого оборудования и средства межсетевого экранирования
- 4) Настроить имеющийся комплект сетевого оборудования и произвести анализ сетевого трафика, передаваемого в сети
- 5) Для существующей сети подобрать средства защиты, обнаружения и реагирования для обеспечения сетевой безопасности

5.2. Критерии оценивания

Критерии оценивания итоговой аттестации:

№	Критерий	Максимальный балл
1	Техническая корректность. Соответствие конфигурации техническому заданию и стандартам. Отсутствие ошибок, которые приведут к неработоспособности. Полнота реализации всех требуемых функций и параметров.	40
2	Безопасность и отказоустойчивость. Реализация принципов безопасности (минимальные привилегии, защита управляющих доступов, шифрование). Учет устойчивости к атакам. Надежность и стабильность конфигурации.	30
3	Эффективность решения. Оптимальность выбранных методов и параметров (метрик OSPF, правил фильтрации). Эффективное использование ресурсов.	30

Максимальный балл за итоговую аттестацию – 100. Менее 50 баллов соответствует оценке «неудовлетворительно», 51-69 баллов соответствуют оценке «удовлетворительно», 70-85 баллов оценке «хорошо», 86-100 баллов оценке «отлично».

Слушатели, получающие высшее образование впервые и(или) среднее профессиональное образование (за исключением лиц, имеющих среднее профессиональное и(или) высшее образование) и отчисленные из образовательной организации (исключением является академический отпуск) не могут продолжать обучение по дополнительной профессиональной программе – программе профессиональной переподготовки.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть программы, выдается справка об обучении или о периоде обучения.

Лицам, завершившим обучение по программе, и успешно прошедшим итоговую аттестацию, присваивается дополнительная квалификация, установленная программой. При освоении программы параллельно с получением высшего образования диплом о профессиональной переподготовке выдается одновременно с получением соответствующего документа об образовании и о квалификации (за исключением лиц, имеющих среднее профессиональное или высшее образование).

Согласовано:

Директор ИДСВО

Руководитель центра «Цифровая кафедра»

И.В. Дарда

В.В. Кокин