Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники»

УТВЕРЖДАЮ
Проректор по УР
_____ А.Г. Балашов
«30» августа 2024 г.

# Дополнительная профессиональная программа (программа профессиональной переподготовки)

## Мониторинг и контроль сетевой безопасности

(наименование программы)

Информационно-коммуникационные технологии

(подвид дополнительного образования)

Москва 2024

## I. Общие положения

1. Дополнительная профессиональная программа (программа профессиональной переподготовки) ИТ-профиля «Мониторинг и контроль сетевой безопасности» (далее – Программа) разработана в соответствии со следующей нормативно правовой основой:

– Федеральный закон от 29 декабря 2012 года №273-ФЗ «Об образовании в Российской Федерации»;

– постановление Правительства Российской Федерации от 13 мая 2021 г. № 729 «О мерах по реализации программы стратегического лидерства «Приоритет-2030»;

– паспорт федерального проекта «Развитие кадрового потенциала ИТ-отрасли» национальной программы «Цифровая экономика Российской Федерации»;

– приказ Минцифры России от 29.12.2023 № 1180 «Об утверждении методик расчета показателей федеральных проектов «Развитие кадрового потенциала ИТ-отрасли» и «Обеспечение доступа в Интернет за счет развития спутниковой связи» национальной программы «Цифровая экономика Российской Федерации», а также внесении изменений в некоторые приказы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» (далее – приказ Минцифры России № 1180);

– приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (с изменениями, внесенными приказом Минобрнауки России о 15 ноября 2013 г. № 1244 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденный приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499»);

– приказ Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов»;

– методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных

стандартов (утв. Минобрнауки России 22 января 2015 г. № ДЛ-1/05вн);

– постановление Правительства Российской Федерации от 11 октября 2023 г. № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

– приказ Минобрнауки России от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

– 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 вместе – 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. (далее – профессиональный стандарт либо профессиональные стандарты).

2. Профессиональная переподготовка заинтересованных лиц (далее – Слушатели), осуществляемая в соответствии с Программой (далее – Подготовка), имеющей отраслевую направленность «Информационно-коммуникационные технологии», проводится в «Национальном исследовательском университете «Московский институт электронной техники» (далее – Университет) в соответствии с учебным планом в очно-заочной форме обучения.

3. Разделы, включенные в учебный план Программы, используются для последующей разработки календарного учебного графика, учебно-тематического плана, рабочей программы, оценочных и методических материалов. Перечисленные документы разрабатываются Университетом самостоятельно, с учетом актуальных положений законодательства об образовании, законодательства в области информационных технологий и смежных областей знаний ФГОС ВО и профессионального стандарта 06.027

«Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

4. Программа регламентирует требования к профессиональной переподготовке в области контроля качества функционирования инфокоммуникационных систем и предоставляемых на их основе сервисов.

Срок освоения Программы составляет 300 ак. часов.

К освоению Программы в рамках проекта допускаются лица:

К обучению по Программе допускаются обучающиеся по очной или по очно-заочной форме за счет бюджетных средств или по договорам об оказании платных образовательных услуг, освоившие программы бакалавриата в объеме не менее 1 курса (бакалавры 2-го курса), специалитета в объеме не менее 1 курса (специалисты 2-го курса) и магистратуры (магистры) по специальностям и направлениям подготовки, отнесённым к ИТ-сфере.

5. Область профессиональной деятельности «Связь, информационные и коммуникационные технологии», уровень 6.

## II. Цель

6. Целью подготовки слушателей по Программе является получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий: администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы; приобретение новой квалификации «Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

## III. Характеристика новой квалификации и связанных с ней видов профессиональной деятельности, трудовых функций и (или) уровней квалификации

7. Виды профессиональной деятельности, трудовая функция, указанные в профессиональном стандарте по соответствующей должности инженер по контролю качества инфокоммуникационных систем, представлены в таблице 1:

**Характеристика новой квалификации, связанной с видом профессиональной деятельности и трудовыми функциями в соответствии с профессиональным стандартом «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»**

| Область профессиональной деятельности | Тип задач профессиональной деятельности | Код и наименование профессиональной компетенции | Трудовые действия | Трудовая функция | Обобщенная трудовая функция | Вид профессиональной деятельности |
|---|---|---|---|---|---|---|
| 06 Связь, информационные и коммуникационные технологии | эксплуатационный | ПК -1 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях | Параметризация операционных систем средств удаленного доступа<br><br>Установка дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация<br><br>Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов)<br><br>Документирование настроек средств обеспечения безопасности удаленного | Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) (D/03.6) | Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения | Администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы |

**Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере, связанной с уровнем формирования и развития в результате освоения Программы «Мониторинг и контроль сетевой безопасности»**

| **Наименование сферы** | **Код и наименование профессиональной компетенции** | **Пример инструментов** | **0 — способность не проявляется/ проявляется в степени, недостаточной для отнесения к 1 уровню сформированности компетенции** | **1 — способность проявляется под внешним контролем / при внешней постановке задачи/ обучающийся пользуется готовыми, рекомендованным и продуктами** | **2 — способность проявляется, но обучающийся эпизодически прибегает к экспертной консультации/ самостоятельно подбирает и пользуется готовыми продуктами** | **3 — способность проявляется системно / обучающийся модифицирует способность под определенные задачи / создает новый продукт, обучает других** |
|---|---|---|---|---|---|---|
| **Мониторинг и контроль сетевой безопасности** | ПК-2 (ID62) Настраивает сетевое оборудование и средства межсетевого экранирования | Cisco, Huawei, С-Терра СиЭсПи, ИнфоТеКС, Zabbix | - | Производит базовую настройку сетевого оборудования при внешней постановке задачи | | - |
| | ПК-3(ID63) Обеспечивает анализ сетевого трафика | Cisco, Huawei, С-Терра СиЭсПи, Snort, Zabbix, Suricata, Vipnet IDS, Wireshark, NetFlow | - | | Производит настройку средств анализа сетевого трафика при помощи эксперта | - |
| | ПК-4(ID64) Участвует в проектировании и | Р 50.1.053-2005, Стандарты ISO | - | | Анализирует схемы информационного | - |

| | | | | | | |
|---|---|---|---|---|---|---|
| | развитии стратегии сетевой безопасности | 27001, ГОСТ Р 50922-2006, Modbus, ГОСТ Р 51188—98, ГОСТ Р 51275-2006, ГОСТ Р ИСО/МЭК 15408 | | | взаимодействия, разрабатывает решения по информационной безопасности объектов сетевой инфраструктуры | |

## IV. Характеристика новых и развиваемых цифровых компетенций, формирующихся в результате освоения программы

8. В ходе освоения Программы Слушателем приобретаются следующие профессиональные компетенции:

- ПК -1 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях.

9. В ходе освоения Программы Слушателем совершенствуются следующие профессиональные компетенции:

- ПК-2 Настраивает сетевое оборудования и средства межсетевого экранирования
- ПК-3 Обеспечивает анализ сетевого трафика
- ПК-4 Участвует в проектировании и развитии стратегии сетевой безопасности.

## V. Планируемые результаты обучения по ДПП ПП

10. 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; приобретение новой квалификации «Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

11. В результате обучения по Программе слушатель сформирует:

**Наименование компетенции:** ПК-1 Способен администрировать программно-аппаратные средства защиты информации в компьютерных сетях

**Знать:** программно-аппаратные средства и методы защиты информации в компьютерных сетях.

**Уметь:** выбирать режимы работы программно-аппаратных средств

защиты информации в компьютерных сетях.

**Иметь навыки:** настройки программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации.

**Наименование компетенции:** ПК-2 Настраивает сетевое оборудование и средства межсетевого экранирования

**Знать:** принципы работы сетевого оборудования; порядок реализации методов и средств межсетевого экранирования; принципы работы и правила эксплуатации применяемых программно-аппаратных средств защиты информации.

**Уметь:** 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;

**Иметь навыки:** настройки сетевого оборудования и средств межсетевого экранирования; управления средствами межсетевого экранирования в компьютерных сетях.

**Наименование компетенции:** ПК-3 Обеспечивает анализ сетевого трафика

**Знать:** 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.

**Уметь:** проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях; производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях; оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях; настраивать средства анализа сетевого трафика.

**Иметь навыки:** 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.

**Наименование компетенции:** ПК-4 Участвует в проектировании и развитии стратегии сетевой безопасности

**Знать:** 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 защите информации.

**Уметь:** 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.

**Иметь навыки:** определения состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях; анализа схемы информационного взаимодействия; разработки решения по информационной безопасности объектов сетевой инфраструктуры.

## VI. Организационно-педагогические условия реализации ДПП

12. Реализация Программы должна обеспечить получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий: «администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы»; приобретение новой квалификации «Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

13. Учебный процесс организуется с применением дистанционных образовательных технологий, инновационных технологий и методик обучения, способных обеспечить получение слушателями знаний, умений и навыков в области контроля качества функционирования инфокоммуникационных систем и предоставляемых на их основе сервисов.

14. Реализация Программы обеспечивается научно-педагогическими кадрами Университета, а также с привлечением к образовательному процессу высококвалифицированных специалистов ИТ-сферы, с обязательным участием представителей профильных организаций-работодателей. Рассматривается возможность привлечения региональных руководителей цифровой трансформации (отраслевых ведомственных и/или корпоративных) к проведению итоговой аттестации, привлечение работников организаций ООО "С-ТЕРРА СИЭСПИ" и ООО «КуРэйт».

## VII. Учебный план ДПП

15. Объем Программы составляет 300 часов

16. Учебный план Программы определяет перечень, последовательность, общую трудоемкость разделов и формы контроля знаний.

Учебный план программы профессиональной переподготовки «Мониторинг и контроль сетевой безопасности»

| № п/п | Наименование раздела (модуля) | Общая трудоемкость (300 часов) | Форма контроля |
|---|---|---|---|
| 1. | Элементы телекоммуникационных сетей | 16 | зачет |
| 2. | Основы системного и сетевого администрирования | 24 | зачет |
| 3. | Инфокоммуникационные системы и сети | 32 | зачет |
| 4. | Безопасность телекоммуникационных систем и сетей | 64 | зачет |
| 5. | Сетевые операционные системы и службы | 16 | зачет |
| 6. | Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности | 48 | зачет |
| 7. | Квантовые технологии обеспечения безопасности сетей | 16 | зачет |
| 8. | Практика | 70 | зачет |
| | Промежуточная аттестация | 6 | зачет |
| | Итоговая аттестация | 8 | Демонстрационный экзамен |
| | Итого: | 300 | |

## VIII. Календарный учебный график

17. Календарный учебный график представляет собой график учебного процесса, устанавливающий последовательность и продолжительность обучения и итоговой аттестации по учебным дням.

Календарный учебный график программы профессиональной переподготовки «Мониторинг и контроль сетевой безопасности»

| № пп | 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 | 38 | 39 | 40 |
| | Входная оценка (ассесмент) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. | Элементы телекоммуникационных сетей | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. | Основы системного и сетевого администрирования | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. | Инфокоммуникационные системы и сети | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. | Безопасность телекоммуникационных систем и сетей | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Промежуточная оценка (ассесмент) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. | Сетевые операционные системы и службы | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6. | Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7. | Квантовые технологии обеспечения безопасности сетей | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8. | Практика | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Промежуточная аттестация | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Итоговая оценка (ассесмент) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | Итоговая аттестация | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

## IX. Рабочая программа учебных предметов, курсов, дисциплин (модулей)

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

Рабочая программа разрабатывается Университетом с учетом профессионального стандарта «Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

| № п/п | Наименование и краткое содержание раздела(модуля) | Объем, часов |
|---|---|---|
| 1. | Элементы телекоммуникационных сетей:<br>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:<br>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 | 24 |
| 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:<br>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 телекоммуникационны х системах, защита от несанкционированного доступа и модели безопасности компьютерных систем, защищенные протоколы стека TCP/IP, исследование защищѐнности сетевых протоколов с использованием средств анализа сетевого трафика, доверенная загрузка вычислительных средств, разработка решений по защите объектов сетевой инфраструктуры | 64 |

| | | |
|---|---|---|
| 5. | Сетевые операционные системы и службы:<br>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:<br>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, | 48 |
| 7. | Квантовые технологии обеспечения безопасности сетей:<br>Квантовая механика для квантовой связи, основы оптики, протоколы квантовой связи, квантовое распределение ключей, основы квантовых повторителей, квантовая запутанность, квантовый интернет, квантовая защита сетей | 16 |
| 8. | **Практика** | 70 |
| 9. | **Промежуточная аттестация** | 6 |
| | **Итоговая аттестация** | 8 |

19. Учебно-тематический план Программы определяет тематическое содержание, последовательность разделов и (или) тем и их трудоемкость.

| № п/п | Наименование раздела(модуля) | Количество часов | | |
|---|---|---|---|---|
| | | аудиторных | | самостоятельной работы (работа с основной и дополнительной литературой, практические задания) |
| | | Лекции | Семинары | |
| 1. | Элементы телекоммуникационных сетей | 8 | - | 8 |
| 2. | Основы системного и сетевого администрирования | 4 | 12 | 8 |

| | | | | |
|---|---|---|---|---|
| 3. | Инфокоммуникационные системы и сети | 16 | 8 | 8 |
| 4. | Безопасность телекоммуникационных систем и сетей | 32 | 16 | 16 |
| 5. | Сетевые операционные системы и службы | 4 | 8 | 4 |
| 6. | Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности | 4 | 32 | 12 |
| 7. | Квантовые технологии обеспечения безопасности сетей | 8 | 4 | 4 |
| 8. | **Практика** | 70 | | |
| 9. | **Промежуточная аттестация** | 6 | | |
| | **Итоговая аттестация** | 8 | | |

## X. Формы аттестации

20. Слушатели, успешно выполнившие все элементы учебного плана, допускаются к итоговой аттестации.

Итоговая аттестация по Программе проводится в форме демонстрационного экзамена.

21. Лицам, успешно освоившим Программу (получивших навыки использования и освоения цифровых технологий, необходимых для выполнения нового вида профессиональной деятельности) и прошедшим итоговую аттестацию в рамках проекта «Цифровые кафедры», выдается документ о квалификации: диплом о профессиональной переподготовке.

При освоении ДПП ПП параллельно с получением высшего образования диплом о профессиональной переподготовке выдается не ранее получения соответствующего документа об образовании и о квалификации (за исключением лиц, имеющих среднее профессиональное или высшее образование).

22. Лицам, не прошедшим процедуры ассесмента и итоговую аттестацию

или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть Программы и (или) отчисленным из Университета, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому Университетом.

## XI. Оценочные материалы

23. Контроль знаний, полученных слушателями при освоении разделов (модулей) Программы, осуществляется в следующих формах:

- текущий контроль успеваемости – обеспечивает оценивание хода освоения разделов Программы, проводится в форме тестов и опросов;

- промежуточная аттестация – завершает изучение отдельного модуля Программы, проводится в форме зачёта;

- итоговая аттестация – завершает изучение всей Программы, проводится в форме демонстрационного экзамена.

24. В ходе освоения Программы каждый слушатель выполняет следующие отчетные работы:

| № п/п | Наименование раздела (модуля) | Задание | Критерии оценки |
|---|---|---|---|
| 1. | Элементы телекоммуникационных сетей | Зачет/Тестирование п.26.1 Кейс задание по классификации сетевого оборудования (п.27.1) | Правильные ответы на 50% и более вопросов теста Корректность классификации оборудования |
| 2. | Основы системного и сетевого администрирования | Зачет/Тестирование (п.26.2))/ Кейс задание по конфигурированию сетевого оборудования (п.27.2) | Правильные ответы на 50% и более вопросов теста Корректность настройки оборудования, последовательность настройки, тестирование и отладка настройки |
| 3. | Инфокоммуникационные системы и сети | Зачет/Тестирование (п.26.3))/ Кейс задание по конфигурированию сетевого оборудования (п.27.3) | Правильные ответы на 50% и более вопросов теста Корректность настройки оборудования, последовательность настройки, тестирование и отладка настройки, наличие анализа альтернативных решений, наличие анализа путей модернизации предложенного решения |
| 4. | Безопасность | Зачет/Тестирование (п.26.4)) | Правильные ответы на 50% и |

| | | | |
|---|---|---|---|
| | телекоммуникационных систем и сетей | Кейс задание по конфигурированию сетевого оборудования (п.27.4) | более вопросов теста<br>Корректность построения модели угроз, настройки оборудования, последовательность настройки, тестирование и отладка настройки |
| 5. | Сетевые операционные системы и службы | Зачет/Тестирование (п.26.5))<br>Кейс задание по конфигурированию сетевого оборудования (п.27.5) | Правильные ответы на 50% и более вопросов теста<br>Корректность построения модели угроз, настройки оборудования, последовательность настройки, тестирование и отладка настройки |
| 6. | Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности | Зачет/Тестирование (п.26.6))<br>Кейс задание по конфигурированию сетевого оборудования (п.27.6) | Правильные ответы на 50% и более вопросов теста<br>Корректность построения модели угроз, настройки оборудования, последовательность настройки, тестирование и отладка настройки |
| 7. | Квантовые технологии обеспечения безопасности сетей | Зачет/Тестирование (п.26.7))<br>Кейс задание по конфигурированию сетевого оборудования (п.27.7) | Правильные ответы на 50% и более вопросов теста<br>Корректность выбора оборудования, методов и протоколов для обеспечения требуемых параметров сети связи. |
| 8. | **Практика** | Зачет/ Кейс задание по настройке сетевого оборудования (п. 27) | Корректность построения модели угроз, настройки оборудования, последовательность настройки, тестирование и отладка настройки, правильность отображения результатов мониторинга сетевой безопасности |
| | **Промежуточная аттестация** | Тестирование (п.26)/Кейс задание по настройке сетевого оборудования (п.27) | Правильные ответы на 50% и более вопросов теста<br>Корректность настройки оборудования, последовательность настройки, тестирование и отладка настройки, наличие анализа альтернативных решений, наличие анализа путей модернизации предложенного решения |
| | **Итоговая аттестация** | Демонстрационный экзамен | Корректность выполнения необходимых подготовительных операции, практической части задания демонстрационного экзамена, правильность оценки результатов анализа или мониторинга |

**25. Текущий контроль. Перечень примерных тестовых заданий**

25.1. Модуль «Элементы телекоммуникационных сетей»

1. 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

25.2 Модуль «Основы системного и сетевого администрирования»

1. Какой тип интерфейса не имеет физического порта, связанного с ним?

а. Консоль

б. Ethernet

в. Последовательный порт

г. Виртуальный интерфейс коммутатора (SVI)

2. Одноранговыми называются сети

а. соединенные через сервер

б. соединенные одним кабелем

в. в которых устройства равноправны

г. в которых используется коммутатором

25.3 Модуль «Инфокоммуникационные системы и сети»

1. 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

2. 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

25.4 Модуль «Безопасность телекоммуникационных систем и сетей»

1. Угроза компьютерной сети – это …

а. вероятное событие

б. детерминированное (всегда определенное) событие

в. событие, происходящее периодически

г. событие, инициируемое руководителем подразделения

2. 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

25.5 Модуль «Сетевые операционные системы и службы»

1. 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

2. 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

25.6 Модуль «Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности»

1. 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

2. 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? (Выберите все подходящие варианты)

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

25.7 Модуль «Квантовые технологии обеспечения безопасности сетей»

1. Какая технологическая особенность лазерного излучения дает теоретическую возможность проведения успешных PNS-атак?

а. Протяженность линий передачи
б. Протокол с измененной конфигурацией состояний
в. Использование многофотонных состояний
г. Собственные шумы системы

2. Какие значения может принимать мера схожести максимально смешанных квантовых состояний?

а. 0
б.1
в. 1/3
г.1/4
д.1/32

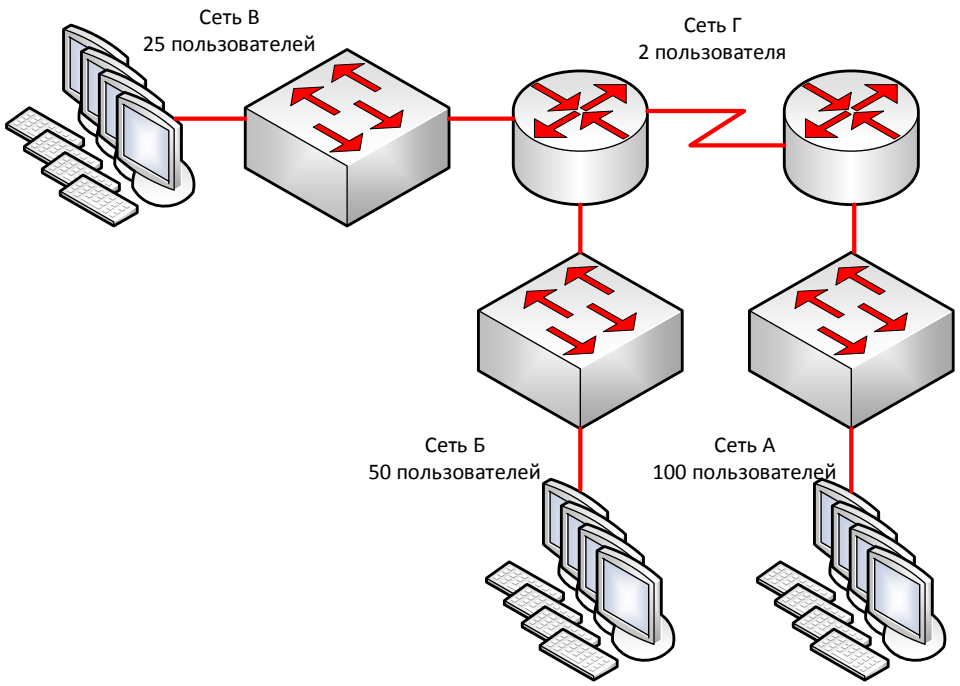
## 26. Промежуточная аттестация. Перечень примерных кейсовых заданий

26.1. Модуль «Элементы телекоммуникационных сетей»

Вариант задания: Провести классификацию выданного оборудования (выдаётся комплект из не менее 5 различного оборудования).

26.2 Модуль «Основы системного и сетевого администрирования»

Вариант задания: Для представленной сети для каждой подсети подобрать наиболее подходящий IP-адрес и префикс так, чтобы все требования к адресации были удовлетворены




26.3 Модуль «Инфокоммуникационные системы и сети»

Вариант задания: 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.

Требования к оформлению, образец оформления:

В отчёте по конфигурированию дать обоснование выбранного типа списка контроля доступа, его конфигурации, привести подтверждения корректности выполнения задания.

26.4 Модуль «Безопасность телекоммуникационных систем и сетей»

Вариант задания: Между двумя пользователями, использующими сеть Интернет необходимо организовать защищенный VoIP канал. Определить модели угроз и произвести настройку оборудования, позволяющего организовать указанный канал.

26.5 Модуль «Сетевые операционные системы и службы»

Вариант задания: 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.

26.6 Модуль «Сетевое администрирование коммутируемых сетей, систем доступа и систем безопасности»
Вариант задания: 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

26.7 Модуль «Квантовые технологии обеспечения безопасности сетей»
Вариант задания: 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.

## 27. Итоговая аттестация. Перечень примерных заданий демонстрационного экзамена

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

## XII. Материально-техническое и учебно-методическое обеспечение Программы

| Наименование специализированных аудиторий, кабинетов, лабораторий | Вид занятия | Наименование оборудования, программного обеспечения |
|---|---|---|
| Учебная аудитория | Лекции | Мультимедиа-проектор Экран, Доска аудиторная, ПЭВМ |
| Компьютерный класс | Семинары (практические | Cisco packet tracer, Cisco Software Development Kit (SDK), Huawei EnSP, |

| | | |
|---|---|---|
| | занятия) | Python, С-Терра СиЭсПи, Snort, Zabbix, Suricata, Vipnet IDS, Wireshark, NetFlow, Linux, Коммутатор Arctika 4804ig. Коммутатор Cisco Catalist 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, С-Терра СиЭсПи, Snort, Zabbix, Suricata, Vipnet IDS, Wireshark, NetFlow, Linux |

## XIII. Список литературы

## 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. 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.
3. 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
4. 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
5. 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.
6. 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.
7. 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: дата обращения: 02.05.2023)

8. 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
9. 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.
10. 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 = Safetyaspects. Guidelinesfortheirinclusioninstandards: 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&section=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. 0106.2020. – М.: Стандартинформ, 2020. - URL: https://docs.cntd.ru/document/573338314 (дата обращения: 02.05.2023). - Режим доступа: по заказу демонстрации.

**Разработчики программы:**

Зав. Кафедрой ТКС, к.т.н. _____ А.А. Бахтин

Доцент каф. ТКС, к.т.н., доцент _____ А.С. Волков

Доцент каф. ТКС, к.т.н., _____ А.Г. Тимошенко

Согласовано:

Зав. Кафедрой ТКС _____ А.А. Бахтин

Директор ДРОП _____ Н.Ю. Соколова

Руководитель проекта
«Цифровые кафедры» _____ В.В. Кокин