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
_____ И.Г.Игнатова
«21» января 2022 г.

ПРОГРАММА ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«ТЕЛЕКОММУНИКАЦИОННЫЕ КВАНТОВЫЕ СИСТЕМЫ И ПЕРСПЕКТИВНЫЕ СЕТИ СВЯЗИ»

Москва, 2022

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Цель программы – формирование у слушателей профессиональных компетенций, необходимых для управления сетевыми системами и устройствами, защиты национальных информационно–телекоммуникационных сетей, обеспечения защиты информации для финансового сектора, государственных органов, крупных технологических компаний и держателей критической информационной инфраструктуры.

Программа адаптирована для обучающихся, проходящих подготовку по направлению подготовки 11.04.04 Электроника и наноэлектроника и рекомендована для студентов программы «Элементная база наноэлектроники» для получения второй для них квалификации, связанной с обслуживанием сетей – это новый виде деятельности необходим для будущей деятельности, которая может учитывать будущее развитие техники связи в том числе квантовых сетей. В рамках программы обучающиеся познакомятся с особенностями настройки и управления сетевых устройств и информационно-коммуникационных систем через решение профессиональных заданий, сформированных производителями сетевого оборудования. В начале каждого модуля используется входное тестирование, на основании которого может быть принято решение о частичной или полной переаттестации по отдельным дисциплинам (Основы сетевой безопасности и Квантовые телекоммуникации), как изученным ранее.

Во время обучения обучающиеся могут сдать сертификационные экзамены (уровней HCIA/CCNA) ведущих производителей телекоммуникационного оборудования (Huawei и Cisco, соответственно). Обучающиеся смогут на практических примерах познакомиться с особенностями проектирования квантово-защищенной сети, видам оборудования, его установки и наладки, интеграции со средствами криптографической защиты информации, для обеспечения требуемых политик информационной безопасности, ознакомиться с доверенным/оконечным узлом магистральной квантовой сети.

1.2. Характеристика нового вида профессиональной деятельности, новой квалификации

Наименование нового вида деятельности: Администрирование информационно-коммуникационных (инфокоммуникационных) систем и Администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы

Область профессиональной деятельности: области инфокоммуникационных технологий, технической поддержки, сетевого и системного администрирования, программирования устройств инфокоммуникационных систем, информационной безопасности инфокоммуникационных систем и/или их составляющих, компьютерных и телекоммуникационных технологий.

Объекты профессиональной деятельности: информационно-коммуникационные системы, квантовые сети

Задачи профессиональной деятельности: Настройка и обслуживание сетевых устройств информационно-коммуникационной системы, администрирование процессами контроля производительности и управления безопасностью сетевых устройств и программного обеспечения, проведение регламентных работ на сетевых устройствах и программном обеспечении инфокоммуникационной системы.

Квалификация: Сетевой инженер

Вид экономической деятельности: деятельность в области информации и связи

Укрупненная группа специальностей: 11.00.00 Электроника, радиотехника и системы связи

1.3. Требования к результатам освоения программы

Планируемые результаты освоения программы:

Обслуживание квантовых линий связи – перспективный расширяющийся сегмент рынка труда. В настоящее время на основе распоряжения Правительства РФ 8.7.2019 № 1484-р головной компанией по развитию квантовых вычислений выступает Госкорпорация «Росатом». Приоритетные отрасли экономики, где будут востребованы слушатели программы: защита национальных информационно–телекоммуникационных сетей, обеспечение защиты информации для финансового сектора, государственных органов, крупных технологических компаний и держателей критической информационной инфраструктуры.

Компетенции определены на основании профессионального стандарта 06.026 «Системный администратор информационно-коммуникационных систем»

Код и формулировка компетенции	**Трудовая функция в соответствии с ПС**		**Индикаторы достижения компетенций**
	Наименование	**Код**	
ПК-1 Способен устанавливать и настраивать сетевое оборудование	Планирование изменений сетевых устройств информационно-коммуникационных систем предметными специалистами из других областей	С/04.6	Знания: протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, международных стандартов локальных вычислительных сетей, инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения сетевых устройств информационно-коммуникационных систем

			Умения: использовать отраслевые стандарты при настройке параметров администрируемых сетевых устройств и программного обеспечения, оценивать риски изменений на сетевых устройствах информационно-коммуникационных систем Опыт деятельности: в конфигурировании параметров администрируемых сетевых устройств и программного обеспечения
ПК-3 Способен находить и устранять неисправности в сети предприятия	Проведение анализа и выявление основных причин сложных проблем, возникающих на сетевых устройствах информационно-коммуникационных систем	С/02.6	Знания: общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, архитектуры аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, базовой эталонной модели взаимодействия открытых систем для управления сетевым трафиком, регламентов проведения профилактических работ на администрируемых сетевых

			устройствах информационно-коммуникационных систем Умения: производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем, конфигурировать операционные системы сетевых устройств, устанавливать и инициализировать новое программное обеспечение сетевых устройств информационно-коммуникационных систем. Опыт деятельности: по исправлению ошибок конфигурации сетевых устройств и операционных систем
ПК-5 Способен администрировать инфраструктуру квантовой сети	Прогнозирование влияния внешних и внутренних воздействий на поведение сетевых устройств информационно-коммуникационной системы	С/06.6	Знания: Методологии и типов изменений инфраструктуры информационных технологий, принципов функционирования аппаратных, программных и программно-аппаратных средств квантовой сети, архитектуры аппаратных, программных и программно-аппаратных средств квантовой сети, применяемые в квантовой сети протоколы. Умения: Оценивать риски и сложности изменения информационно-коммуникационной системы, управлять процессом

			изменения сетевых устройств, производить оценку воздействия изменения на поведение информационно-коммуникационной системы Опыт деятельности: в определении критериев оптимизации производительности квантовой сети

Компетенции определены на основании профессионального стандарта 06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»

Код и формулировка компетенции	**Трудовая функция в соответствии с ПС**		**Индикаторы достижения компетенций**
	Наименование	**Код**	
ПК-2 Способен управлять сетью для поддержки необходимого уровня производительности противодействия угрозам, уменьшения количества инцидентов безопасности	Коррекция производительности сетевой инфокоммуникационной системы	C/04.6	Знания: модели ISO для управления сетевым трафиком, моделей OSI, IEEE, средств защиты от несанкционированного доступа, модели управления сетью Умения: использовать современные средства контроля производительности администрируемой сети, настраивать параметры современных программно-аппаратных межсетевых экранов Опыт деятельности: в модификации части администрируемой сети
ПК-4 Способен	Планирование	E/04.6	Знания: принципов

производить модернизацию сети	модернизации сетевых устройств		функционирования сетевых аппаратных средств, архитектура сетевых аппаратных средств, технологии в сетевом администрировании, рекомендации производителей сетевого оборудования, Умения: применять современные инфокоммуникационные технологии, обосновывать предложения по реализации стратегии в области инфокоммуникационных технологий Опыт деятельности: в планировании работ по развертыванию, конфигурированию и эксплуатации сетевых устройств
ЦК-1 Способен обеспечивать безопасность сетей и сетевого оборудования	Определение параметров безопасности и защиты программного обеспечения сетевых устройств	D/01.6	Знания: классификации операционных систем согласно классам безопасности, средств защиты от несанкционированного доступа операционных систем и систем управления базами данных, защищенные протоколы управления, основные средства криптографии Умения: пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Опыт деятельности: в оценке и планированию

			безопасности и защиты программного обеспечения сетевых устройств от несанкционированного доступа

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

Наличие высшего образования или получающие высшее образование (при наличии соответствующей справки с указанием года окончания) по направлениям подготовки инженерного дела, технологий, технических, математических и естественных наук.

Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

1.5. Трудоемкость обучения

Нормативная трудоемкость обучения по данной программе – 250 часов, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя.

1.6. Форма обучения

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

1.7. Режим занятий

Без отрыва от работы

При любой форме обучения учебная нагрузка устанавливается не более 54 часов в неделю, включая все виды аудиторной и внеаудиторной (самостоятельной) учебной работы слушателя. Продолжительность одного часа занятий 45 минут.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план программы переподготовки

№ п/п	Наименование учебных дисциплин (модулей)	Общая трудоемкость, час	Контактная работа, час				ЭО или ДОТ, час				СРС, час	Промежуточная аттестация
			Всего	Лекции	Лабораторные занятия	Практические занятия	Всего	Лекции	Лабораторные занятия	Практические занятия		
1.	Введение в сетевые технологии	16	-	-	-	-	8	8	-	-	8	За
2.	Основы построения сетей и систем	32	-	-	-	-	16	8	-	8	16	За
3.	Основы сетевой безопасности	30	-	-	-	-	14	10	-	4	16	За
4.	Сетевое и системное администрирование	16	-	-	-	-	8	2	-	6	8	За
5.	Квантовые телекоммуникации	14	-	-	-	-	6	2	-	4	8	За
6.	Практика	125	-	-	-	-	57	-	48	9	68	За
6.1	Маршрутизация и коммутация / Сетевые технологии от Cisco Systems	34	-	-	-	-	18	-	16	2	16	За
6.2	Сетевая безопасность/Аналитика в области кибербезопасности	57	-	-	-	-	21	-	16	5	36	За
6.3	Беспроводные технологии/Программно-конфигурируемые сети/Сетевое программирование	34	-	-	-	-	18	-	16	2	16	За
7	Консультации	11	-	-	-	-	11	-	-	-	-	-
8	Итоговая аттестация - *Итоговый экзамен*	6	6	-	-	-	-	-	-	-	-	Экз
	Итого по программе	250	6	-	-	-	120	30	48	31	124	-

2.2. Календарный учебный график

Мес	Февраль					Март					Апрель					Май					Июнь					Июль					Сентябрь					Октябрь					Ноябрь					Декабрь				
Числа	1-6	7 - 13	14 - 20	21 - 27	28-6	7 - 13	14 - 20	21 - 27	28 - 3	4 - 10	11 - 17	18 - 24	25 - 1	2 - 8	9 - 15	16 - 22	23 - 29	30 - 5	6 - 12	13 - 19	20 - 26	27 - 3	4 - 10	11 - 17	18 - 24	Каникулы	1-4	5 - 11	12 - 18	19 - 25	26 - 2	3 - 9	10 - 16	17 - 23	24 - 30	31 - 6	7 - 13	14 - 20	21 - 27	28 - 4	5 - 11	12 - 18	19 - 25	26 - 31
БвСТ																																															
ОПСиС																																															
ССБ																																															
СиСА																																															
КТ																																															
МиК/СТ																																															
СБ/АвОК																																															
БТ/ПКС/СП																																															
																																														ИА	

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

3.1. Рабочая программа учебной дисциплины «Введение в сетевые технологии»

3.1.1. Цели и задачи дисциплины (модуля)

Обучающиеся смогут познакомиться с основами теории работы сетевых технологий и отдельных сетевых протоколов, актуальных стандартах сетей связи, принципами модернизации сетевой инфраструктуры, планированием защиты сети от несанкционированного доступа.

3.1.2. Требования к результатам освоения учебной дисциплины (модуля)

Планируемые результаты освоения программы:

Дисциплина (модуль) участвует в формировании компетенций: ПК-4 Способен производить модернизацию сети и ЦК-1 Способен обеспечивать безопасность сетей и сетевого оборудования

В результате изучения дисциплины обучающийся должен иметь:

Знания: основы построения сетей связи, стандарты и протоколы, основы защиты сети от несанкционированного доступа

Умения: применять современные инфокоммуникационные технологии

3.1.3. Учебно-тематический план дисциплины

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Введение в сетевые технологии. Основы телекоммуникаций**	14	-	-	-	8	-	-	6
1.1	Этапы развития сетей связи и их классификация. Стандартизация в области телекоммуникаций	8	-	-	-	4	-	-	4
1.2.	Специализированные сети связи, назначение и	6	-	-	-	4	-	-	2

	технологии								
2.	Промежуточная аттестация – Зачёт	2	-	-	-	-	-	-	2
	Всего	16	-	-	-	8	-	-	8

3.1.4. Содержание дисциплины

Перечень лекций

Номер раздела и темы	Краткое содержание	Количество часов
1.1	Понятие первичной, вторичной сетей связи. Сети доступа и транспортные сети, технологии транспортных сетей. Классификация сетей связи и сетевых технологий. Основные институты и организации стандартизации сетевых технологий. Модель взаимодействия OSI. Модель TCP/IP.	4
1.2	Специализированные сети связи, назначение и технологии. Нормативная и правовая база. Архитектура сети. Применение и назначение сетей	4

3.1.5. Учебно-методическое и информационное обеспечение дисциплины

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. Управление безопасностью критических информационных инфраструктур : учебное пособие / А. Н. Петухов, П. Л. Пилюгин, А. В. Душкин, Ю. А. Губсков ; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ"; под редакцией А.В. Душкина. - Москва : МИЭТ, 2021. - 208 с.
4. Бахтин А.А., Волков А.С., Муратчаев С.С. Имитационное моделирование сетей связи в среде Network Simulator-3: учебное пособие. – М.: МИЭТ, 2018. – 61 с.

3.1.6. Материально-техническое обеспечение дисциплины

Для доступа к ресурсам дисциплины у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по дисциплине.

Программное обеспечение по дисциплине: Cisco Packet Tracer, GNS3, eNSP

3.1.7. Система контроля и оценивания

Перед прохождением дисциплины (модуля) проводится входное тестирование, выполняемое за ограниченное время с ограничением попыток (1 попытка), которые определяют уровень знаний обучающегося.

Оценка качества освоения дисциплины (модуля) включает промежуточную аттестацию обучающихся, которая проводится в форме тестирования по дисциплине. Тестирование проводится в moodle. Время тестирование ограничено, количество попыток: 2. Вопросы тестирования содержат как вопросы закрытого типа, так и вопросы открытого типа. Для успешного прохождения дисциплины обучающемуся необходимо набрать не менее 70 % за тест по дисциплине. Текущее тестирование, в том числе встроенное в теоретические материалы не влияет на оценку качества, а является вспомогательным и позволяет студенту получить доступ к соответствующим разделам дисциплины (модуля), либо вернуться к изучаемому материалу для повторного ознакомления с ним.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.2. Рабочая программа учебной дисциплины «Основы построения сетей и систем»

3.2.1. Цели и задачи дисциплины (модуля)

Обучающиеся смогут познакомиться с основами теории построения и эксплуатации телекоммуникационных сетей и систем, влиянием помех на каналы связи, принципами работы телефонных сетей связи, а также методами коммутации каналов связи.

3.2.2. Требования к результатам освоения учебной дисциплины (модуля)

Планируемые результаты освоения программы:

Дисциплина (модуль) участвует в формировании компетенций: ПК-4 Способен производить модернизацию сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: структурных и функциональных схем телекоммуникационных сетей

Умения: анализировать возможные варианты решения поставленной задачи

Опыт деятельности: эскизного проектирования систем связи по заданному набору характеристик

3.2.3. Учебно-тематический план дисциплины

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Физические основы телекоммуникационных систем»**	16	-	-	-	4	-	4	8
1.1	Телекоммуникационные сети	2	-	-	-	2	-	-	-
1.2.	Помехи в каналах связи	2	-	-	-	2	-	-	-
1.3	Исследование моделей канала. Исследование цифровой модуляции	12	-	-	-	-	-	4	8
2.	**Построение телекоммуникационных систем»**	14	-	-	-	4	-	4	6
2.1	Телефонные сети связи	2	-	-	-	2	-	-	-
2.2	Каналообразующие устройства	2	-	-	-	2	-	-	-
2.3	Исследование способов доступа к среде	10	-	-	-	-	-	4	6
3.	Промежуточная аттестация - Зачёт	2	-	-	-	-	-	-	2
	Всего	**32**	-	-	-	**8**	-	**8**	**16**

3.2.4. Содержание дисциплины

Перечень лекций

Номер раздела и темы	Краткое содержание	Количество часов
1.1	Телекоммуникации и связь. Основные понятия. Разновидности сетей. Телекоммуникационные сети. Классификация сигналов. Их параметры. Многоканальные телекоммуникационные	2

	системы. Глазковая диаграмма и ее параметры. Динамический диапазон, пик-фактор и другие параметры сигналов	
1.2	Помехи в каналах связи. Потери в каналах связи. Канал с АБГШ, ДСК. Релеевский и райсовский каналы. Эффективность использования мощности и полосы пропускания при модуляции	2
2.1	Взаимоувязанная сеть связи РФ. Телефонные сети связи. Принципы и аппаратура телефонной передачи. Аппаратура системы радиосвязи. Интерфейс открытых систем	2
2.2	Каналообразующие устройства. Методы коммутации. Кодеки и модемы.	2

Перечень практических занятий

Номер раздела и темы	**Наименование практического занятия**	**Количество часов**
1.3	Исследование моделей канала. Исследование цифровой модуляции	4
2.3	Исследование способов доступа к среде	4

3.2.5. Учебно-методическое и информационное обеспечение дисциплины

1. А.Л. Бузова, Специальная радиосвязь. Развитие и модернизация оборудования и объектов [Текст]: Монография / Под ред. А.Л. Бузова, С.А. Букашкина. - М.: Радиотехника, 2017. - 448 с. - ISBN 978-5-93108-159-5: 301-00, 500 экз.
2. Галкин В.А. (Автор МИЭТ, МРТУС). Системы связи с подвижными объектами в среде системного моделирования System Vue [Текст] Лабораторный практикум / В.А. Галкин; Министерство образования и науки РФ, Национальный исследовательский университет "МИЭТ". - М.: МИЭТ, 2016. - 108 с. - Имеется электронная версия издания. - б.ц., 70 экз.
3. Галкин В.А. (Автор МИЭТ, МРТУС). Цифровая мобильная радиосвязь [Текст]: Учеб. пособие / В.А. Галкин. - 2-е изд., перераб. и доп. - М.: Горячая линия-Телеком, 2012. - 584 с. - URL: https://e.lanbook.com/book/5143#book_name (дата обращения: 01.09.2019). - ISBN 978-5-9912-0185-8: 1049-17; 1048-94, 500 экз.

3.2.6. Материально-техническое обеспечение дисциплины

Для доступа к ресурсам дисциплины у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по дисциплине.

Программное обеспечение по дисциплине: Cisco Packet Tracer, GNS3, eNSP

3.2.7. Система контроля и оценивания

Перед прохождением дисциплины (модуля) проводится входное тестирование, выполняемое за ограниченное время с ограничением попыток (1 попытка), которые определяют уровень знаний обучающихся и необходимость дополнительного изучения материала дисциплины.

Оценка качества освоения дисциплины (модуля) включает промежуточную аттестацию обучающихся, которая проводится в форме тестирования по дисциплине. Тестирование проводится в moodle. Время тестирование ограничено, количество попыток: 2. Вопросы тестирования содержат как вопросы закрытого типа, так и вопросы открытого типа. Для успешного прохождения дисциплины обучающемуся необходимо набрать не менее 70 % за тест по дисциплине. Текущее тестирование, в том числе встроенное в теоретические материалы не влияет на оценку качества, а является вспомогательным и позволяет студенту получить доступ к соответствующим разделам дисциплины (модуля), либо вернуться к изучаемому материалу для повторного ознакомления с ним.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.3. Рабочая программа учебной дисциплины (модуля) «Основы сетевой безопасности»

3.3.1. Цели и задачи дисциплины (модуля)

Дисциплина (модуль) направлены на формирование знаний методологических и алгоритмических основ, стандартов, механизмов и сервисов сетевой безопасности, основ криптографических алгоритмов и протоколов, проблем информационной безопасности в сети интернет, основных алгоритмов шифрования, принципов распределения открытых ключей. При изучении дисциплины (модуля) обучающиеся познакомятся с методами оценки безопасности и защиты приложений от несанкционированного доступа, основам планирования защиты операционных систем от несанкционированного доступа, оценкой защиты операционных систем от несанкционированного доступа, параметризации операционных систем средств удаленного доступа.

3.3.2. Требования к результатам освоения учебной дисциплины (модуля)

Планируемые результаты освоения программы:

Дисциплина (модуль) участвует в формировании компетенций: ЦК-1 Способен обеспечивать безопасность сетей и сетевого оборудования

В результате изучения дисциплины обучающийся должен иметь:

Знания: классификации операционных систем согласно классам безопасности, средств защиты от несанкционированного доступа операционных систем и систем управления базами данных, защищенные протоколы управления, основные средства криптографии

Умения: пользоваться нормативно-технической документацией в области инфокоммуникационных технологий

3.3.3. Учебно-тематический план дисциплины

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Общие вопросы безопасности сетей**	9				3		2	4
1.1	Взаимосвязь современных понятий в области защиты информации.	2				0,4		1	0,6
1.2	Модели угроз информационным технологиям	2				0,9			1,1
1.3	Риск ориентированный подход к обеспечению безопасности информационных технологий	2				0,4		1	0,6
1.4	Система нормативных документов по защите информации. Основные отечественные, зарубежные и международные документы	2				0,9			1,1
1.5	Формирование требований по защите информации на примере требований к объектам критической инфраструктуры	1				0,4			0,6
2.	**Элементы сетевой безопасности**	6				2			4
2.1.	Введение в управление доступом. Понятия идентификации и	2				0,6			1,4

	аутентификации. Дискреционное и мандатное управление доступом.								
2.2.	Модели безопасности вычислительных систем. Субъектно-объектная модель безопасности вычислительных систем.	2				0,7			1,3
2.3.	Понятие доверенной вычислительной среды. Доверенная загрузка	2				0,7			1,3
3.	**Основы криптографии**	8				3		1	4
3.1.	Основные понятия криптографии. Симметричные криптографические алгоритмы. Алгоритмы Магма, Кузнечик и AES	2				0,8		0,5	0,7
3.2.	Криптографические алгоритмы хеширования. Алгоритмы SHA и Стрибог	2				0,7			1,3
3.3	Ассиметричные криптографические алгоритмы. Алгоритм RSA. Электронная цифровая подпись.	2				0,7			1,3
3.4	Инфраструктура открытых ключей.	2				0,8		0,5	0,7
4	**Технологии защиты сетей**	6				2		1	3
4.1.	Архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем	2				0,5		0,5	1
4.2	Стек протоколов TCP/IP и защищенные протоколы в этом стеке. Протокол IPSec	1				0,5			0,5
4.3	Стек протоколов TCP/IP и защищенные протоколы в этом стеке. Протокол TLS	1				0,5			0,5

4.4	Современные средства защиты от несанкционированного доступа и защиты сетевого трафика	2				0,5		0,5	1
5	Промежуточная аттестация: Зачёт	-	-	-	-	-	-	-	1
	Всего	30				10		4	16

3.3.4. Содержание дисциплины

Перечень лекций

Номер раздела и темы	Краткое содержание	Количество часов
1.1	Взаимосвязь современных понятий в области защиты информации.	0,4
1.2	Модели угроз информационным технологиям	0,9
1.3	Риск ориентированный подход к обеспечению безопасности информационных технологий	0,4
1.4	Система нормативных документов по защите информации. Основные отечественные, зарубежные и международные документы	0,9
1.5	Формирование требований по защите информации на примере требований к объектам критической инфраструктуры	0,4
2.1	Введение в управление доступом. Понятия идентификации и аутентификации. Дискреционное и мандатное управление доступом.	0,6
2.2	Модели безопасности вычислительных систем. Субъектно-объектная модель безопасности вычислительных систем.	0,7
2.3	Понятие доверенной вычислительной среды. Доверенная загрузка	0,7
3.1	Основные понятия криптографии. Симметричные криптографические алгоритмы. Алгоритмы Магма, Кузнечик и AES	0,8
3.2	Криптографические алгоритмы хеширования. Алгоритмы SHA и Стрибог	0,7
3.3	Ассиметричные криптографические алгоритмы. Алгоритм RSA. Электронная цифровая подпись.	0,7
3.4	Инфраструктура открытых ключей.	0,8
4.1	Архитектура защиты информации в соответствии с базовой	0,5

	эталонной моделью взаимодействия открытых систем	
4.2	Стек протоколов TCP/IP и защищенные протоколы в этом стеке. Протокол IPSec	0,5
4.3	Стек протоколов TCP/IP и защищенные протоколы в этом стеке. Протокол TLS	0,5
4.4	Современные средства защиты от несанкционированного доступа и защиты сетевого трафика	0,5

Перечень практических занятий

Номер раздела и темы	**Наименование практического занятия**	**Количество часов**
1.1	Взаимосвязь современных понятий в области защиты информации.	1
1.3	Риск ориентированный подход к обеспечению безопасности информационных технологий	1
3.1	Основные понятия криптографии. Симметричные криптографические алгоритмы. Алгоритмы Магма, Кузнечик и AES	0,5
3.4	Инфраструктура открытых ключей.	0,5
4.1	Архитектура защиты информации в соответствии с базовой эталонной моделью взаимодействия открытых систем	0,5
4.4	Современные средства защиты от несанкционированного доступа и защиты сетевого трафика	0,5

3.3.5. Учебно-методическое и информационное обеспечение дисциплины

1. 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: 21.12.2020). - ISBN 978-5-94774-821-5

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2017. - 384 с. - ISBN 978-5-4383-0135-6

3. 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: 21.12.2020). - ISBN 978-5-9912-0147-6.

4. 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.

3.3.6. Материально-техническое обеспечение дисциплины

Для доступа к ресурсам дисциплины у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по дисциплине.

Программное обеспечение по дисциплине: Cisco Packet Tracer, GNS3, eNSP, Kali Linux, С-Терра Клиент А ST, С-Терра Шлюз DP ST, С-Терра Юнит, Zabbix

3.3.7. Система контроля и оценивания

Перед прохождением дисциплины (модуля) проводится входное тестирование, выполняемое за ограниченное время с ограничением попыток (1 попытка), которые определяют возможность получения перезачёта по дисциплине (модулю) или необходимость дополнительного изучения материала дисциплины. Перезачёт по дисциплине (модулю) допускается, если обучающийся правильно ответил на 70 % и более.

Оценка качества освоения дисциплины (модуля) включает промежуточную аттестацию обучающихся, которая проводится в форме тестирования по дисциплине. Тестирование проводится в moodle. Время тестирование ограничено, количество попыток: 2. Вопросы тестирования содержат как вопросы закрытого типа, так и вопросы открытого типа. Для успешного прохождения дисциплины обучающемуся необходимо набрать не менее 70 % за тест по дисциплине. Текущее тестирование, в том числе встроенное в теоретические материалы не влияет на оценку качества, а является вспомогательным и позволяет студенту получить доступ к соответствующим разделам дисциплины (модуля), либо вернуться к изучаемому материалу для повторного ознакомления с ним.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.4. Рабочая программа учебной дисциплины «Сетевое и системное администрирование»

3.4.1. Цели и задачи дисциплины (модуля)

Обучающиеся смогут познакомиться с основами теории работы сетевых технологий и отдельных сетевых протоколов, принципами работы сетевого оборудования и его конфигурации, сетевых топологий

3.4.2. Требования к результатам освоения учебной дисциплины (модуля)

Планируемые результаты освоения программы:

Дисциплина (модуль) участвует в формировании компетенций: ПК-5 Способен администрировать инфраструктуру квантовой сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: Методологии и типов изменений инфраструктуры информационных технологий, основы сетевых технологий, принципы работы сетевого оборудования, архитектуры аппаратных, программных и программно-аппаратных средств сети
Умения: работа с инфокоммуникационными системами и сетевым оборудованием
Опыт деятельности: в конфигурации сетевого оборудования, владении документацией

3.4.3. Учебно-тематический план дисциплины

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Коммутация и маршрутизация в сетях связи. Сетевые протоколы**	14	-	-		2	-	6	6
1.1	Сетевые операционные системы. Сетевые соединения, топологии сетей связи	2	-	-	-	2	-	-	-
1.2.	Маршрутизация в IP сетях	2	-	-		-		2	-
1.3	Сегментация локальных сетей	10	-	-	-	-	-	4	6
2.	Промежуточная аттестация - Зачёт	2	-	-	-	-	-	-	2
	Всего	**16**	-	-		**2**	-	**6**	**8**

3.4.4. Содержание дисциплины

Перечень лекций

Номер раздела и темы	Краткое содержание	Количество часов
1.1	Сетевые операционные системы. Сетевые соединения, топологии сетей связи. Стандарты беспроводных сетей связи	2

Перечень практических занятий

Номер раздела и темы	Наименование практического занятия	Количество часов
1.2	Маршрутизация в IP сетях	2
1.3	Сегментация локальных сетей	4

3.4.5. Учебно-методическое и информационное обеспечение дисциплины

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей : Пер. с англ. / К. Закер. - СПб. : BHV, 2002. - 988 с.
2. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : Питер, 2014. - 960 с. - (Классика Computer Science).
3. Казаков Ф.А.Администрирование локальных сетей и телекоммуникационных систем: Учеб. пособие / Ф.А. Казаков, Ф.А. Кузьмин. - Томск : СПБ Графикс, 2012. - 157 с.

3.4.6. Материально-техническое обеспечение дисциплины

Для доступа к ресурсам дисциплины у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по дисциплине.

Программное обеспечение по дисциплине: Cisco Packet Tracer, GNS3, eNSP.

3.4.7. Система контроля и оценивания

Перед прохождением дисциплины (модуля) проводится входное тестирование, выполняемое за ограниченное время с ограничением попыток (1 попытка), для определения уровня знаний студентов по изучаемым темам дисциплины (модуля).

Оценка качества освоения дисциплины (модуля) включает промежуточную аттестацию обучающихся, которая проводится в форме тестирования по дисциплине. Тестирование проводится в moodle. Время тестирование ограничено, количество попыток: 2. Вопросы тестирования содержат как вопросы закрытого типа, так и вопросы открытого типа. Для успешного прохождения дисциплины обучающемуся необходимо набрать не менее 70 % за тест по дисциплине. Текущее тестирование, в том числе встроенное в теоретические материалы не влияет на оценку качества, а является вспомогательным и позволяет студенту получить доступ к соответствующим разделам дисциплины (модуля), либо вернуться к изучаемому материалу для повторного ознакомления с ним.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.5. Рабочая программа учебной дисциплины «Квантовые телекоммуникации»

3.5.1. Цели и задачи дисциплины (модуля)

Обучающиеся смогут познакомиться с основами квантовых технологий, квантовой криптографии, введению в протоколы квантового распределения ключа и квантовую связь; понять, какую роль играют квантовые коммуникационные сети в инфраструктуре связи и какие ограничения накладывает применяемое сетевое оборудование применяемые квантовые технологии.

3.5.2. Требования к результатам освоения учебной дисциплины (модуля)

Планируемые результаты освоения программы:

Дисциплина (модуль) участвует в формировании компетенций: ПК-5 Способен администрировать инфраструктуру квантовой сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: основы квантовых технологий и квантовой криптографии, инфраструктуру квантовых сетей, принципов функционирования аппаратных, программных и программно-аппаратных средств квантовой сети, архитектуры аппаратных, программных и программно-аппаратных средств квантовой сети, применяемые в квантовой сети протоколы

Умения: Оценивать риски и сложности изменения информационно-коммуникационной системы

3.5.3. Учебно-тематический план дисциплины

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Основы квантовых технологий и квантовой криптографии**	2	-	-	-	-	-	1	1
1.1	Концепция квантовой криптографии	0,4	-	-	-	-	-	0,2	0,2
1.2.	Передача информации по квантовым каналам. Квантовые шумы и квантовая коррекция	0,8	-	-	-	-	-	0,4	0,4

	ошибок								
1.3.	Протоколы квантового распределения ключей: E91, B92, BB84, Lo05, SARG04, 4+2, COW, DPS	0,8	-	-	-	-	-	0,4	0,4
2.	**Инфраструктура квантовых сетей**	2	-	-	-	-	-	2	-
2.1.	Нормативно-правовое регулирование квантовых сетей	0,4	-	-	-	-	-	0,4	-
2.2.	Квантовая сеть на примере квантовой линии связи Москва-Санкт-Петербург	1	-	-	-	-	-	1	-
2.3.	Недостатки и перспективы развития квантовых сетей	0,6	-	-	-	-	-	0,6	-
3.	**Принципы функционирования и архитектура аппаратных, программных и программно-аппаратных средств квантовых сетей**	4	-	-	-	1	-	2	1
3.1.	Оборудование для квантовых сетей	2				0,6		0,9	0,5
3.2.	Программное обеспечение для квантовых сетей	2				0,4		1,1	0,5
4	**Протоколы квантовых сетей**	4	-	-		1	-	1	2
4.1.	Протоколы для передачи данных в квантовых сетях	2	-	-		0,5	-	0,5	1
4.2	Протоколы для управления квантовыми сетями	2	-	-		0,5	-	0,5	1
6.	Промежуточная аттестация: зачёт	2	-	-	-	-	-	-	2
	Всего	14			-	2		4	8

3.5.4. Содержание дисциплины

Перечень лекций

Номер раздела и темы	**Краткое содержание**	**Количество часов**
3.1	Оборудование для квантовых сетей: оборудование оптических	0,6

	сетей, спутниковые квантовые сети, приёмники, передатчики, квантовые генераторы случайных числе, дополнительное оборудование.	
3.2	Программное обеспечение для квантовых сетей. Управление квантовым оборудованием, мониторинг состояния квантового и телекоммуникационного оборудования. Программно-конфигурируемые сети.	0,4
4.1	Стандартные протоколы ВОЛС: Ethernet-100 BASE-F, Ethernet-1000 BASE-SX, ATM, FDDI LSF, Fiber Channel, 10GBASE-E и 10GBASE-L	0,5
4.2	Протоколы для управления сетевыми устройствами: SNMP, NETCONF, SSH, Telnet, HTTP, HTTPs, OpenFlow.	0,5

Перечень практических занятий

Номер раздела и темы	**Наименование практического занятия**	**Количество часов**
1.1	Введение в квантовые технологии. Криптография с открытым ключом. Квантовое распределение ключа.	0,2
1.2	Передача информации по квантовым каналам. Квантовые шумы и квантовая коррекция ошибок.	0,4
1.3	Протоколы квантового распределения ключей: E91, B92, BB84, Lo05, SARG04, 4+2, COW, DPS	0,4
2.1	Нормативно-правовое регулирование квантовых сетей	0,4
2.2	Квантовая сеть на примере квантовой линии связи Москва-Санкт-Петербург	1
2.3	Недостатки и перспективы развития квантовых сетей. Влияние сетевой инфраструктуры на квантовую передачу. Современные решения, позволяющие увеличить дальность квантовой коммуникации.	0,6
3.1	Практические примеры применения оборудования для квантовых сетей. Подходы проектирования квантово-защищенной сети, виды оборудования, его установки и наладки	0,9
3.2	Интеграция оборудования со средствами криптографической защиты информации, для обеспечения требуемых политик информационной безопасности	1,1
4.1	Подходы к проектированию квантово-защищенной сети, виды оборудования, его установки и наладки, интеграция со средствами криптографической защиты информации, для	0,5

	обеспечения требуемых политик информационной безопасности	
4.2	Тенденции развития квантового мира: криптомиграция вычислительной техники, киберстрахование, инфраструктура как услуга (Iaas) и удалённое управление, доверие оконечных устройств, квантовое лидерство.	0,5

3.5.5. Учебно-методическое и информационное обеспечение дисциплины

1. Дорожная карта квантовые коммуникации. - URL: https://digital.ac.gov.ru/ (дата обращения: 24.12.2021)

2. Сухоручкина И.Н. КВАНТОВЫЕ КОММУНИКАЦИОННЫЕ СЕТИ В ИНФРАСТРУКТУРЕ СВЯЗИ // Россия: тенденции и перспективы развития. 2021. №16-2. - URL: https://cyberleninka.ru/article/n/kvantovye-kommunikatsionnye-seti-v-infrastrukture-svyazi (дата обращения: 25.12.2021).

3. Козубов А.В., Гайдаш А.А., Кынев С.М., Егоров В.И., Иванова А.Е., Глейм А.В., Мирошниченко Г.П. Основы квантовой коммуникации. Часть 1: Учебно-методическое пособие. - Санкт-Петербург: Университет ИТМО, 2019. - URL: https://books.ifmo.ru/ (дата обращения: 24.12.2021)

4. ITU Workshop on Quantum Information Technology (QIT) for Networks - URL: https://www.itu.int/ (дата обращения: 24.12.2021)

3.5.6. Материально-техническое обеспечение дисциплины

Для доступа к ресурсам дисциплины у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по дисциплине.

Программное обеспечение по дисциплине: Cisco Packet Tracer, GNS3, eNSP.

3.5.7. Система контроля и оценивания

Перед прохождением дисциплины (модуля) проводится входное тестирование, выполняемое за ограниченное время с ограничением попыток (1 попытка), которые определяют возможность получения перезачёта по дисциплине (модулю) или необходимость дополнительного изучения материала дисциплины. Перезачёт по дисциплине (модулю) допускается, если обучающийся правильно ответил на 70 % и более.

Оценка качества освоения дисциплины (модуля) включает промежуточную аттестацию обучающихся, которая проводится в форме тестирования по дисциплине. Тестирование проводится в moodle. Время тестирование ограничено, количество попыток: 2. Вопросы тестирования содержат как вопросы закрытого типа, так и вопросы открытого типа. Для успешного прохождения дисциплины обучающемуся необходимо набрать не менее 70 % за тест по дисциплине. Текущее тестирование, в том числе встроенное в теоретические материалы не влияет на оценку качества, а является вспомогательным и позволяет студенту

получить доступ к соответствующим разделам дисциплины (модуля), либо вернуться к изучаемому материалу для повторного ознакомления с ним.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.6. Рабочая программа практики «Маршрутизация и коммутация»

3.6.1. Цели и задачи практики

В практике у обучающихся будут сформированы базовые знания сетевых технологий и основные навыки поддержки небольших сетей предприятия, построенных с применением оборудования Huawei. После изучения дисциплины обучающиеся смогут:

- Описывать базовые принципы сетевого IP взаимодействия.
- Планировать IP адресацию.
- Выполнять базовые операции в VRP.
- Описывать функции и принципы работы коммутационного оборудования.
- Настраивать рабочую сеть с применением коммутаторов и протоколов STP/RSTP.
- Описывать основные принципы работы протоколов маршрутизации, настраивать протокол OSPF для организации эффективно работающей сети.
- Настраивать популярные сетевые сервисы, такие как DHCP, FTP и telnet для эффективного управления сетью.
- Настраивать агрегацию линков и технологию VLAN для повышения производительности сети 2 уровня.
- Настраивать HDLC, PPP и PPPoE в распределенных сетях.
- Выполнять конфигурацию технологии NAT.
- Настраивать ACL, AAA и IPSec для защиты инфраструктуры IP сетей.
- Конфигурировать протокол SNMP для обеспечения централизованного мониторинга сетевого оборудования.

3.6.2. Требования к результатам освоения практики

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ПК-1 Способен устанавливать и настраивать сетевое оборудование и ПК-5 Способен администрировать инфраструктуру квантовой сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, международных стандартов локальных вычислительных сетей, инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения сетевых устройств информационно-коммуникационных систем

Умения: использовать отраслевые стандарты при настройке параметров администрируемых сетевых устройств и программного обеспечения, оценивать риски изменений на сетевых устройствах информационно-коммуникационных систем, управлять процессом изменения сетевых устройств, производить оценку воздействия изменения на поведение информационно-коммуникационной системы

Опыт деятельности: в конфигурировании параметров администрируемых сетевых устройств и программного обеспечения компании Huawei; в определении критериев оптимизации производительности сети

3.6.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Построение простейших IP-сетей**	2						1	1
1.1	Технологии и среды передачи данных	0,2						0,1	0,1
1.2.	Семейство стандартов Ethernet	0,3						0,2	0,1
1.3.	Основы IPv4	0,4						0,2	0,2
1.4	Вспомогательные протоколы ICMPv4 и ARP	0,4						0,2	0,2
1.5	Протоколы транспортного уровня	0,4						0,2	0,2
1.6	Пример обмена данными между сетевыми узлами	0,3						0,1	0,2
2.	**Настройка устройств Huawei**	4					2		2
2.1.	Основы VRP. Обзор линеек оборудования Huawei. Виртуальные роутер AR1000v и ЦОД-коммутатор CloudEngine 12800	1					0,5		0,5
2.2.	Навигация в командной строке CLI	1					0,5		0,5
2.3.	Управление файловой системой и навигация в ней	1					0,5		0,5
2.4.	Управление образом операционной системы	1					0,5		0,5

	VRP. Использование FTP и TFTP. Настройки операционной системы								
3.	**Поддержка локальных корпоративных сетей**	3					1,5		1,5
3.1.	Построение коммутируемой сети. Базовые настройки коммутации (Развертывание сети с одним коммутатором)	1					0,5		0,5
3.2.	Протокол связующего дерева (Spanning Tree Protocol)	1					0,5		0,5
3.3.	Протокол быстрого связующего дерева RSTP (Rapid Spanning Tree Protocol)	1					0,5		0,5
4	**Обеспечение межсетевого взаимодействия**	4					2		2
4.1.	Сегментация IP-сети	1					0,5		0,5
4.2.	Статические маршруты IP	1					0,5		0,5
4.3.	Дистанционно-векторная маршрутизация с помощью протокола RIP	1					0,5		0,5
4.4	Маршрутизация по состоянию канала с помощью протокола OSPF	1					0,5		0,5
5.	**Внедрение прикладных сервисов**	3					1,5		1,5
5.1.	Принципы функционирования протокола DHCP. Настройка DHCP-сервера на маршрутизаторе Huawei и DHCP-клиента на сетевых интерфейсах	1					0,5		0,5
5.2.	Принципы функционирования протокола FTP. Настройка FTP-сервера и авторизации	1					0,5		0,5

	пользователей на маршрутизаторе Huawei								
5.3.	Принципы функционирования протокола Telnet. Настройка доступа к сетевому оборудованию Huawei по telnet	1					0,5		0,5
6.	**Технологии коммутации в локальных сетях**	3					2		1
6.1.	Объединение физ.интерфейсов (Link aggregation) и протокол LACP	0,7					0,5		0,2
6.2.	Использование VLAN (access/trunk/hybrid – порты) и VVLAN	0,8					0,5		0,3
6.3.	Устаревшие протоколы GARP и GVRP	0,7					0,5		0,2
6.4.	Маршрутизация между VLAN	0,7					0,5		0,2
6.5.	Wireless LAN Overview	0,1							0,1
7.	**Глобальные сети**	2						0,5	1,5
7.1.	HDLC и связанные с ним протоколы – PPP	1						0,25	0,75
7.2.	DSL и использование PPPoE. Настройка PPPoE	1						0,25	0,75
8.	**Контроль доступа, AAA и ACL**	3					2,5		0,5
8.1	Частные и публичные адреса. Трансляция адресов	0,6					0,5		0,1
8.2	Классификация и фильтрация трафика	0,6					0,5		0,1
8.3	AAA (Authentication, Authorization, Accounting) Базовая настройка	0,6					0,5		0,1
8.4	Защита трафика с помощью IPSec VPN. Создание IPSec	0,6					0,5		0,1
8.5	GRE (Generic Routing Encapsulation). Туннели.	0,6					0,5		0,1
9.	**Основы управления**	3					2		1

	сетями								
9.1.	Протокол SNMP – Simple Network Management Protocol, настройка и управление	1,5					1		0,5
9.2.	Huawei eSight	1,5					1		0,5
10.	**Ipv6-сети**	2						1	1
10.1	Преимущества протокола Ipv6	0,4						0,2	0,2
10.2	Маршрутизация в Ipv6 – статическая и OSPFv3	0,8						0,4	0,4
10.3	Распределение Ipv6-адресов – DHCPv6	0,8						0,4	0,4
11.	**Основы MPLS и Segment Routing**	4					2,5	0,5	1
11.1	Принципы работы MPLS в режимах коммутации ячеек/кадров	0,9					0,6	0,1	0,2
11.2	MPLS TE и MPLS VPN	1					0,6	0,1	0,3
11.3	Что такое SR (Segment Routing) и зачем он нужен. Проблемы LDP/RSVP и их решение.	1,1					0,7	0,2	0,2
11.4	IS-IS SR	1					0,6	0,1	0,3
12.	Промежуточная аттестация: зачёт								1
	Всего	34					16	2	16

3.6.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	**Наименование лабораторного занятия**	**Количество часов**
2.1.	Основы VRP. Обзор линеек оборудования Huawei. Виртуальные роутер AR1000v и ЦОД-коммутатор CloudEngine 12800	0,5
2.2.	Навигация в командной строке CLI	0,5
2.3.	Управление файловой системой и навигация в ней	0,5
2.4.	Управление образом операционной системы VRP. Использование FTP и TFTP. Настройки операционной системы	0,5
3.1.	Построение коммутируемой сети. Базовые настройки	0,5

	коммутации (Развертывание сети с одним коммутатором)	
3.2.	Протокол связующего дерева (Spanning Tree Protocol)	0,5
3.3.	Протокол быстрого связующего дерева RST	0,5
4.1.	Сегментация IP-сети	0,5
4.2.	Статические маршруты IP	0,5
4.3.	Дистанционно-векторная маршрутизация с помощью протокола RIP	0,5
4.4	Маршрутизация по состоянию канала с помощью протокола OSPF	0,5
5.1.	Принципы функционирования протокола DHCP. Настройка DHCP-сервера на маршрутизаторе Huawei и DHCP-клиента на сетевых интерфейсах	0,5
5.2.	Принципы функционирования протокола FTP. Настройка FTP-сервера и авторизации пользователей на маршрутизаторе Huawei	0,5
5.3.	Принципы функционирования протокола Telnet. Настройка доступа к сетевому оборудованию Huawei по telnet	0,5
6.1.	Объединение физ.интерфейсов (Link aggregation) и протокол LACP	0,5
6.2.	Использование VLAN (access/trunk/hybrid – порты) и VVLAN	0,5
6.3.	Устаревшие протоколы GARP и GVRP	0,5
6.4.	Маршрутизация между VLAN	0,5
8.1	Частные и публичные адреса. Трансляция адресов	0,5
8.2	Классификация и фильтрация трафика	0,5
8.3	AAA (Authentication, Authorization, Accounting) Базовая настройка	0,5
8.4	Защита трафика с помощью IPSec VPN. Создание IPSec	0,5
8.5	GRE (Generic Routing Encapsulation). Туннели.	0,5
9.1.	Протокол SNMP – Simple Network Management Protocol, настройка и управление	1
9.2.	Что такое Huawei eSight	1
11.1	Принципы работы MPLS в режимах коммутации ячеек/кадров	0,6

11.2	MPLS TE и MPLS VPN	0,6
11.3	Что такое SR (Segment Routing) и зачем он нужен. Проблемы LDP/RSVP и их решение.	0,7
11.4	IS-IS SR	0,6

Перечень практических занятий

Номер раздела и темы	Наименование практического занятия	Количество часов
1.1	Технологии и среды передачи данных	0,1
1.2.	Семейство стандартов Ethernet	0,2
1.3.	Основы Ipv4	0,2
1.4	Вспомогательные протоколы ICMPv4 и ARP	0,2
1.5	Протоколы транспортного уровня	0,2
1.6	Пример обмена данными между сетевыми узлами	0,1
7.1.	HDLC и связанные с ним протоколы – PPP	0,25
7.2.	DSL и использование PPPoE. Настройка PPPoE	0,25
10.1	Преимущества протокола Ipv6	0,2
10.2	Маршрутизация в Ipv6 – статическая и OSPFv3	0,4
10.3	Распределение Ipv6-адресов – DHCPv6	0,4
11.1	Принципы работы MPLS в режимах коммутации ячеек/кадров	0,1
11.2	MPLS TE и MPLS VPN	0,1
11.3	Что такое SR (Segment Routing) и зачем он нужен. Проблемы LDP/RSVP и их решение.	0,2
11.4	IS-IS SR	0,1

3.6.5. Учебно-методическое и информационное обеспечение дисциплины

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей : Пер. с англ. / К. Закер. – СПб. : BHV, 2002. – 988 с.
2. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – СПб. : Питер, 2014. – 960 с. – (Классика Computer Science).
3. Казаков Ф.А.Администрирование локальных сетей и телекоммуникационных систем: Учеб. Пособие / Ф.А. Казаков, Ф.А. Кузьмин. – Томск : СПБ Графикс, 2012. – 157 с.

3.6.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и

аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: Huawei AR1000v, Huawei CloudEngine 12800, Huawei eNSP Lab.

3.6.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.7. Рабочая программа практики «Сетевые технологии от Cisco Systems»

3.7.1. Цели и задачи практики

Практика формирует знания, умения и опыт необходимые для базовой настройки и эксплуатации сетей Cisco и позволяет научить:

- Определять компоненты компьютерной сети и описывать их основные характеристики
- Понимать модель взаимодействия хостов в системе
- Описывать функции и особенности ОС Cisco Internetwork Operating System (IOS®)
- Понимать, что такое локальная сеть, для чего используются коммутаторы
- Разбираться в принципах работы технологии канального уровня Ethernet и в принципах работы коммутаторов
- Совершать первоначальную настройку коммутаторов
- Описывать сетевой уровень стека TCP/IP, разбираться в принципах Ipv4-адресации
- Описывать функции транспортного и прикладного уровней
- Понимать функции маршрутизации
- Совершать первоначальную настройку маршрутизаторов
- Объяснять процесс взаимодействия хостов при передаче трафика через коммутаторы и маршрутизаторы
- Выявлять и устранять распространенные проблемы, которые могут возникнуть в локальной сети или в работе коммутаторов

- Описывать преимущества и возможности адресного пространства IPv6
- Разбираться в преимуществах и ограничениях статической маршрутизации
- Понимать принципы работы технологии VLAN, уметь настраивать на устройствах Cisco
- Понимать, как настроить маршрутизацию между VLAN
- Объяснять основы протоколов динамической маршрутизации, разбираться в терминологии Open Shortest Path First (OSPF)
- Понимать логику работы протоколов Spanning Tree Protocol (STP) и Rapid Spanning Tree Protocol (RSTP)
- Настраивать агрегацию каналов с помощью технологии EtherChannel
- Описывать протоколы резервирования шлюзов (протоколы группы FHRP)
- Разбираться на базовом уровне в работе технологий WAN и VPN
- Настраивать списки контроля доступа (ACL)
- Внедрять технологию Dynamic Host Configuration Protocol (DHCP) и использовать трансляции сетевых адресов (Network Address Translation) для подключения корпоративной сети к Интернету
- Описывать базовые концепции QoS
- Разбираться в принципах построения беспроводных сетей, знать основные архитектуры, понимать преимущества использования контроллеров Wireless LAN Controllers (WLCs)
- Описывать архитектуру сети и устройства, понимать принципы виртуализации
- Описывать преимущества и возможности Software-Defined Networking (SDN), знать решения для интеллектуального управления сетью, например, Cisco DNA Center™, Software-Defined Access (SD-Access), и Software-Defined Wide Area Network (SD-WAN)
- Пользоваться основными инструментами мониторинга ОС IOS
- Понимать принципы управления сетевыми устройствами
- Описывать текущий ландшафт угроз безопасности
- Описывать основные технологии защиты от угроз
- Внедрять механизмы безопасного управления сетевыми устройствами
- Совершать рекомендуемые базовые настройки безопасности

3.7.2. Требования к результатам освоения практики

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ПК-1 Способен устанавливать и настраивать сетевое оборудование и ПК-5 Способен администрировать инфраструктуру квантовой сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, международных стандартов локальных вычислительных сетей, инструкции по установке и эксплуатации администрируемых сетевых устройств и программного обеспечения сетевых устройств информационно-коммуникационных систем

Умения: использовать отраслевые стандарты при настройке параметров администрируемых сетевых устройств и программного обеспечения, оценивать риски изменений на сетевых устройствах информационно-коммуникационных систем, управлять процессом изменения

сетевых устройств, производить оценку воздействия изменения на поведение информационно-коммуникационной системы

Опыт деятельности: в конфигурировании параметров администрируемых сетевых устройств и программного обеспечения компании Cisco; в определении критериев оптимизации производительности сети

3.7.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Коммутация в сетях**	8,5					4	0,5	4
1.1	Практические вопросы коммутации	1,5						0,5	1
1.2.	Конфигурирование коммутаторов	7					4		3
2.	**Маршрутизация в сетях**	8,5					4	0,5	4
2.1.	Практические вопросы маршрутизации	1,5						0,5	1
2.2.	Конфигурирование маршрутизаторов	7					4		3
3.	**Управление в сети**	8,5					4	0,5	4
3.1.	Практические вопросы управления сетевыми ресурсами	1,5						0,5	1
3.2.	Управление сетевыми ресурсами	7					4		3
4	**Настройка безопасного доступа в сети**	7,5					4	0,5	3
4.1.	Практические вопросы настройки безопасного доступа к сети	1,5						0,5	1
4.2	Управление безопасным сетевым доступом	7					4		2
5.	Промежуточная аттестация:	1							1

	Зачёт								
	Всего	34					16	2	16

3.7.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	Наименование лабораторного занятия	Количество часов
1.2	Начало работы с интерфейсом командной строки. Анализ работы коммутатора. Базовые настройки коммутатора. Реализация начальной конфигурации коммутатора. Анализ работы прикладного уровня TCP/IP. Анализ процесса передачи пакетов. Устранение неполадок в работе коммутатора. Анализ проблем, которые могут возникнуть из-за настроек дуплекса порта.	4
2.2	Настройки интерфейса маршрутизатора. Внедрение протоколов Layer 2 Discovery. Реализация начальной конфигурации маршрутизатора. Настройка шлюза по умолчанию. Базовые настройки IPv6. Статические маршруты IPv4. Статические маршруты IPv6. Внедрение VLAN и Trunk. Поиск и устранение неполадок в работе технологий VLAN и Trunk. Настройки маршрутизатора для обеспечения маршрутизации между VLAN. Настройки сети среднего размера с несколькими VLAN. Настройка Single-Area OSPF. Использование технологии EtherChannel.	4
3.2	Базовые настройки IPv4 ACL. Внедрение нумерованных и именованных IPv4 ACL. Настройка адресов, полученных от провайдера. Статический NAT. Внедрение Dynamic NAT и Port Address Translation (PAT). Начало работы с WLC. Мониторинг WLC. Настройка Dynamic (VLAN) Interface. Настройка DHCP Scope. Создание и настройка WLAN. Использование Remote Access Dial-In User Service (RADIUS) сервера для безопасного доступа. Исследование функций управления. Исследование Cisco DNA™ Center. Настройка и проверка работы протокола NTP. Настройка логирования. Создание Cisco IOS Image Backup. Обновление ОС Cisco IOS	4
4.2	Настройка типа безопасности сети Wi-Fi Protected Access 2 (WPA2) Pre-shared Key (PSK) для WLAN в GUI. Настройка безопасного удаленного доступа, защита консольного доступа. Ограничение удаленного доступа. Настройка механизма Port Security. Внедрение базовых настроек безопасности.	4

Перечень практических занятий

Номер раздела и темы	Наименование практического занятия	Количество часов
1.1	Описание функций сети. Модель взаимодействия устройств сети. Функции и возможности ОС Cisco IOS. Введение в локальные сети. Принципы работы технологии Ethernet, функции канального уровня стека TCP/IP. Базовая конфигурация коммутатора. Обзор сетевого уровня стека TCP/IP, принципы IPv4-адресации. Обзор транспортного и прикладного уровней стека TCP/IP.	0,5
2.1	Описание функций маршрутизации. Базовая конфигурация маршрутизатора Cisco. Описание процесса передачи пакетов между двумя хостами в сети. Статическая и динамическая маршрутизация. Технологии VLAN и Trunk. Поиск и устранение неполадок в работе простой сети. Введение в IPv6. Маршрутизация между VLAN. Компоненты протокола OSPF.	0,5
3.1	Улучшение характеристик работы избыточных коммутируемых топологий с помощью технологии EtherChannel. Управление трафиком с использованием ACL. Подключение корпоративной сети к Интернету. Анализ возможностей Software-Defined Networking (SDN), решения для интеллектуального управления сетью. Инструменты мониторинга ОС IOS	0,5
4.1	Безопасное управление сетевыми устройствами. Механизмы безопасного доступа. Рекомендуемые базовые настройки безопасности	0,5

3.7.5. Учебно-методическое и информационное обеспечение дисциплины

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей : Пер. с англ. / К. Закер. - СПб. : BHV, 2002. - 988 с.
2. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : Питер, 2014. - 960 с. - (Классика Computer Science).
3. Казаков Ф.А.Администрирование локальных сетей и телекоммуникационных систем: Учеб. пособие / Ф.А. Казаков, Ф.А. Кузьмин. - Томск : СПБ Графикс, 2012. - 157 с.

3.7.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: Cisco Packet Tracer.

3.7.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.8. Рабочая программа практики «Сетевая безопасность»

3.8.1. Цели и задачи практики

Практика направлена на формирование у обучающихся знаний умений и опыта работы в области сетевой безопасности. Обучающиеся смогут:

- Описывать базовые концепции информационной безопасности
- Знать распространенные типы сетевых атак
- Понимать, как обеспечивать безопасность процесса эксплуатации и обслуживания устройств
- Использовать различные методы анализ защищенности и методы сбора статистических данных
- Понимать основные принципы работы межсетевых экранов
- Понимать технологию трансляции сетевых адресов
- Использовать базовые механизмы защиты сетевых устройств
- Знать компоненты операционной системы
- Перечислять методы защиты операционных систем
- Описывать принципы шифрования
- Использовать шифрование прикладного уровня

3.8.2. Требования к результатам освоения практики

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ЦК-1 Способен обеспечивать безопасность сетей и сетевого оборудования и ПК-2 Способен управлять сетью для

поддержки необходимого уровня производительности противодействия угрозам, уменьшения количества инцидентов безопасности

В результате изучения дисциплины обучающийся должен иметь:

Знания: средств защиты от несанкционированного доступа операционных систем и систем управления базами данных

Умения: использовать различные методы анализ защищенности и методы сбора статистических данных

Опыт деятельности: в оценке и планированию безопасности и защиты программного обеспечения сетевых устройств от несанкционированного доступа на оборудовании Huawei

3.8.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Обзор информационной безопасности**	8					2	1	5
1.1	Понятия информационной безопасности	4						1	3
1.2.	Настройки безопасности в TCP/IP.	4					2		2
2.	**Анализ защищенности**	10					3	1	6
2.1.	Инциденты безопасности	4						1	3
2.2.	Мониторинг и анализ защищенности сети	6					3		3
3.	**Основы сетевой безопасности**	13					4	1	8
3.1.	Межсетевые экраны	5						1	4
3.2.	Настройка межсетевых экранов на сетевом оборудовании	8					4		4
4	**Безопасность ОС и оконечных устройств**	12					3	1	8
4.1.	Оконечное оборудование	5						1	4
4.2	Настройка межсетевых	7					3		4

	экранов на пользовательском оборудовании								
5	**Сервисы шифрования**	13					4	1	8
5.1	Криптография и VPN	5						1	4
5.2	Настройка VPN	8					4		4
6.	Промежуточная аттестация: Зачёт	1							1
	Всего	57					16	5	36

3.8.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	**Наименование лабораторного занятия**	**Количество часов**
1.2	Настройки безопасности в TCP/IP.	2
2.2	Мониторинг и анализ данных. Проактивный анализ. Пассивный сбор данных. Анализ данных. Процедура развертывания системы безопасности	3
3.2	Настройка межсетевых экранов на сетевом оборудовании	4
4.2	Настройка межсетевых экранов на пользовательском оборудовании под управлением ОС: Windows/ Linux Operating System.	3
5.2	Настройка VPN. IPSec VPN. SSL VPN.	4

Перечень практических занятий

Номер раздела и темы	**Наименование практического занятия**	**Количество часов**
1.1	Базовые сетевые концепции. Архитектура сетей TCP/IP. Распространенные сетевые протоколы. Стандарты и рекомендации. Стандарты информационной безопасности. ISO 27001 ISMS. Распространенные сетевые устройства. Базовые сетевые устройства. Первичный вход на устройство. Тенденции развития защиты от угроз и информационной безопасности. Защита от угроз. Тенденции развития информационной безопасности. Распространенные угрозы информационной безопасности. Обзор текущей ситуации. Безопасность приложений. Основные понятия	1

	информационной безопасности. Риски и активы.	
2.1	Аварийное реагирование на инцидент безопасности. Процесс реагирования на инцидент безопасности. Цифровая криминалистика. Киберпреступность. Обзор цифровой криминалистики. Процесс криминалистики. Рекомендации и лучшие практики, разбор сценариев. Распространенные сценарии.	1
3.1	Управление пользователями межсетевых экранов (МСЭ). Пользовательская аутентификация и сервисы AAA. Управление процессом аутентификации. Обзор IPS. Обзор систем предотвращения вторжений. Обзор сетевого антивируса. Введение в межсетевые экраны. Обзор МСЭ. Политики инспектирования. ASPF. Резервирование. Dual-System Hot Standby. Network Address Translation. Принципы трансляции сетевых адресов NAT. Source NAT.	1
4.1	МСЭ оконечного оборудования и антивирусное ПО. Windows Firewalls. Linux Firewalls. Антивирусное ПО. Обзор операционной системы. Распространенные типы серверов и угроз. Обзор серверных платформ. Серверное ПО. Распространенные атаки и уязвимости.	1
5.1	Public Key Infrastructure (PKI) Certificate System. Цифровые сертификаты. Структура PKI. Механизмы криптографии. Основы криптографии. Обзор VPN. Шифрование и дешифрование. Алгоритмы шифрования. Распространенные современные алгоритмы. Безопасность терминального оборудования.	1

3.8.5. Учебно-методическое и информационное обеспечение дисциплины

1. 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: 21.12.2020). - ISBN 978-5-94774-821-5

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2017. - 384 с. - ISBN 978-5-4383-0135-6

3. 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: 21.12.2020). - ISBN 978-5-9912-0147-6.

4. 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.

3.8.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: Huawei AR1000v, Huawei CloudEngine 12800, Huawei eNSP Lab, HiSec Insight, Policy Center.

3.8.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.9. Рабочая программа практики «Аналитика в области кибербезопасности»

3.9.1. Цели и задачи практики

Программа знакомит слушателя с основными теоретическими принципами безопасности и дает практические навыки, необходимые для установки, устранения неполадок и мониторинга сетевых устройств и позволяющие поддерживать целостность, конфиденциальность и доступность данных и устройств. Обучающиеся смогут: разработать политику безопасности сети, оценить возможные угрозы и эффективно бороться с ними, получите навыки по обеспечению безопасности сетевого периметра и сетевых устройств всех уровней; получить опыт работы с современной сетью и научиться пользоваться технологиями в сфере сетевой безопасности, в том числе с технологиями AAA, Firewall, VPN.

3.9.2. Требования к результатам освоения практики

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ЦК-1 Способен обеспечивать безопасность сетей и сетевого оборудования и ПК-2 Способен управлять сетью для

поддержки необходимого уровня производительности противодействия угрозам, уменьшения количества инцидентов безопасности

В результате изучения дисциплины обучающийся должен иметь:

Знания: средств защиты от несанкционированного доступа операционных систем и систем управления базами данных

Умения: использовать различные методы анализ защищенности и методы сбора статистических данных

Опыт деятельности: в оценке и планированию безопасности и защиты программного обеспечения сетевых устройств от несанкционированного доступа на оборудовании Cisco

3.9.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Безопасность сети и сетевых устройств**	8					2	1	5
1.1	Фундаментальные принципы безопасной сети. Безопасность Сетевых устройств OSI	3						1	2
1.2.	Настройка основных параметров безопасности граничного маршрутизатора	5					2		3
2.	**Авторизация, аутентификация и учет доступа (AAA)**	10					3	1	6
2.1.	Свойства AAA. Локальная AAA аутентификация. Server-based AAA	3						1	2
2.2.	Защита административного доступа с помощью модели AAA и протокола RADIUS	7					3		4
3.	**Реализация технологий брандмауэра**	13					4	1	8

3.1.	ACL. Технология брандмауэра. Контекстный контроль доступа. Политики брандмауэра основанные на зонах.	5						1	4
3.2.	Внедрение зонального межсетевого экрана (Zone-Based Policy Firewall) на пограничном маршрутизаторе	8					4		4
4	**Технологии предотвращения вторжения**	12					3	1	8
4.1.	IPS. Локальные сети. Безопасности второго уровня. Беспроводные сети. VoIP и SAN.	2						0,3	1,7
4.2	Криптографические системы	2						0,3	1,7
4.3	Технологий VPN	2						0,4	1,6
4.4	Внедрение Site-to-Site VPN с помощью интерфейса командной строки на маршрутизаторах Cisco	6					3		3
5	**Межсетевой экран**	13					4	1	8
5.1	Введение в адаптивное устройство безопасности ASA. Управление безопасной сети	5						1	4
5.2	Настройка Cisco ASA	8					4		4
6	Промежуточная аттестация: Зачёт	1							1
	Всего	57					16	5	36

3.9.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	**Наименование лабораторного занятия**	**Количество часов**
1.2.	Настройка основных параметров безопасности граничного маршрутизатора	2

2.2.	Защита административного доступа с помощью модели AAA и протокола RADIUS	3
3.2.	Внедрение зонального межсетевого экрана (Zone-Based Policy Firewall) на пограничном маршрутизаторе	4
4.4	Внедрение Site-to-Site VPN с помощью интерфейса командной строки на маршрутизаторах Cisco	3
5.2	Настройка Cisco ASA	4

Перечень практических занятий

Номер раздела и темы	**Наименование практического занятия**	**Количество часов**
1.1	Фундаментальные принципы безопасной сети. Безопасность Сетевых устройств OSI	1
2.1.	Свойства AAA. Локальная AAA аутентификация. Server-based AAA	1
3.1.	ACL. Технология брандмауэра. Контекстный контроль доступа. Политики брандмауэра основанные на зонах.	1
4.1.	IPS. Локальные сети. Безопасности второго уровня. Беспроводные сети. VoIP и SAN.	0,3
4.2	Криптографические системы	0,3
4.3	Технологий VPN	0,4
5.1	Введение в адаптивное устройство безопасности ASA. Управление безопасной сети	1

3.9.5. Учебно-методическое и информационное обеспечение дисциплины

1. 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: 21.12.2020). - ISBN 978-5-94774-821-5

2. Бутакова Н.Г. Криптографические методы и средства защиты информации: Учеб. пособие / Н.Г. Бутакова, Н.В. Федоров. - СПб. : ИЦ "Интермедия", 2017. - 384 с. - ISBN 978-5-4383-0135-6

3. 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: 21.12.2020). - ISBN 978-5-9912-0147-6.

4. 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.

3.9.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: Cisco packet tracer, Cisco TrustSec, Cisco ASA, Cisco Security Manager.

3.9.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.10. Рабочая программа практики «Беспроводные технологии»

3.10.1. Цели и задачи практики

Программа знакомит с основами топологии, номенклатурой оборудования и принципами построения беспроводных сетей предприятия с использованием оборудования Huawei, а также с основами планирования, настройки, оптимизации беспроводных сетей предприятия, централизованного управления беспроводными сетями с помощью сервиса мониторинга и управления eSight и способами поиска неисправностей в беспроводных сетях. Практические занятия позволяют освоить основные команды конфигурации беспроводных контроллеров и различных точек доступа в режиме командной строки и с помощью web интерфейса. Программа включает дополнительную информацию по особенностям стандарта 802.11 ax

Формирование базовых знаний и навыков, необходимых для установки и настройки беспроводного оборудования Huawei, а также планирования, оптимизации и поиска неисправностей в беспроводных сетях предприятия.

3.10.2. Требования к результатам освоения практики

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ПК-3 Способен находить и устранять неисправности в сети предприятия и ПК-4 Способен производить модернизацию сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, архитектуры аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, базовой эталонной модели взаимодействия открытых систем для управления сетевым трафиком, регламентов проведения профилактических работ на администрируемых сетевых устройствах информационно-коммуникационных систем

Умения: производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем, конфигурировать операционные системы сетевых устройств, устанавливать и инициализировать новое программное обеспечение сетевых устройств информационно-коммуникационных систем.

Опыт деятельности: по исправлению ошибок конфигурации сетевых устройств и операционных систем, конфигурированию и эксплуатации сетевых устройств

3.10.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Базовые настройки точек доступа**	5,4					2	0,4	3
1.1	Применение оборудования Huawei WLAN	2						0,4	1,6
1.2.	Настойка базовых атрибутов контроллера АС. Обновление ПО контроллеров и точек	3,4					2		1,4

	доступа. Настройка консольного пользовательского интерфейса. Настройка удаленного доступа. Проверка настроек. Анализ работы туннеля CAPWAP									
2.	**Продвинутые настройки точек доступа**	6,4					3	0,4	3	
2.1.	Сетевые особенности БЛВС	2						0,4	1,6	
2.2.	Использование и настройка VLAN в беспроводной инфраструктуре. Настройка канального и сетевого уровней беспроводной сети	4,4					3		1,4	
3.	**Безопасность беспроводных сетей**	6,4					3	0,4	3	
3.1.	Безопасное подключение клиентов	2						0,4	1,6	
3.2.	Настройка безопасного доступа. Конфигурация RADIUS-серверов. Настройка шифрования	4,4					3		1,4	
4	**Планирования БЛВС**	7,4					4	0,4	3	
4.1.	Физические аспекты планирования БЛВС	2						0,4	1,6	
4.2	Планирование БЛВС. Балансировка нагрузки. Huawei WLAN Planner	5,4					4		1,4	
5	**Настройка и обслуживание БЛВС**	7,4					4	0,4	3	
5.1	eSight и обзор Wizard Configuration.	2						0,4	1,6	
5.2	Сетевое управление и поиск неисправностей	5,4					4		1,4	
5.	Промежуточная аттестация: Зачёт	1							1	
	Всего	34					16	2	16	

3.10.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	Наименование лабораторного занятия	Количество часов
1.2	Настойка базовых атрибутов контроллера АС. Обновление ПО контроллеров и точек доступа. Настройка консольного пользовательского интерфейса. Настройка удаленного доступа. Проверка настроек. Анализ работы туннеля CAPWAP	2
2.2	Использование и настройка VLAN в беспроводной инфраструктуре. Настройка канального и сетевого уровней беспроводной сети	3
3.2	Настройка безопасного доступа. Конфигурация RADIUS-серверов. Настройка шифрования	3
4.2	Планирование БЛВС. Балансировка нагрузки. Huawei WLAN Planner	4
5.2	Система сетевого управления eSight. Настройка точек доступа. Поиск неисправностей	4

Перечень практических занятий

Номер раздела и темы	Наименование практического занятия	Количество часов
1.1	Применение оборудования Huawei WLAN	0,4
2.1	Сетевые особенности БЛВС	0,4
3.1	Безопасное подключение клиентов. Роуминг	0,4
4.1	Процесс планирования БЛВС. Характеристики антенн. Интерференция. Технология балансировки нагрузки Huawei. Huawei WLAN Planner	0,4
5.1	eSight и обзор Wizard Configuration. Радиопрофили. Методология поиска и устранения неполадок.	0,4

3.10.5. Учебно-методическое и информационное обеспечение дисциплины

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей : Пер. с англ. / К. Закер. - СПб. : BHV, 2002. - 988 с.
2. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : Питер, 2014. - 960 с. - (Классика Computer Science).
3. Казаков Ф.А.Администрирование локальных сетей и телекоммуникационных систем:

Учеб. пособие / Ф.А. Казаков, Ф.А. Кузьмин. - Томск : СПБ Графикс, 2012. - 157 с.

3.10.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: CAPWAP, Huawei WLAN Planner, eSight.

3.10.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.11. Рабочая программа практики «Программно-конфигурируемые сети»

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ПК-3 Способен находить и устранять неисправности в сети предприятия и ПК-4 Способен производить модернизацию сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, архитектуры аппаратных, программных и программно-

аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, базовой эталонной модели взаимодействия открытых систем для управления сетевым трафиком, регламентов проведения профилактических работ на администрируемых сетевых устройствах информационно-коммуникационных систем

Умения: производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем, конфигурировать операционные системы сетевых устройств, устанавливать и инициализировать новое программное обеспечение сетевых устройств информационно-коммуникационных систем.

Опыт деятельности: по исправлению ошибок конфигурации сетевых устройств и операционных систем, конфигурированию и эксплуатации сетевых устройств

3.11.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Платформа маршрутизации**	5,4					2	0,4	3
1.1	Основы Huawei VRP	2						0,4	1,6
1.2.	Основные команды и функциональные клавиши интерфейса командной строки	3,4					2		1,4
2.	**IP-адресация**	6,4					3	0,4	3
2.1.	Протокол сетевого уровня и IP-адресация	2						0,4	1,6
2.2.	Расчет IP-сети и IP-подсети, Планирование IP-адресов сети	4,4					3		1,4
3.	**Настройка оборудования**	6,4					3	0,4	3
3.1.	Составление и формирование таблицы MAC-адресов	2						0,4	1,6

3.2.	Агрегация каналов Ethernet и стекирование коммутаторов	4,4					3		1,4
4	**Программно-конфигурируемые сети**	7,4					4	0,4	3
4.1.	Управление сетью. Основы SDN и NFV	2						0,4	1,6
4.2	Решение NMS и O&M на основе SDN. Решения Huawei NFV	5,4					4		1,4
5	**Сетевое программирование**	7,4					4	0,4	3
5.1	Сетевое программирование и автоматизация	2						0,4	1,6
5.2	Внедрение сетевой автоматизации. Спецификации кодирования Python	5,4					4		1,4
6.	Промежуточная аттестация: Зачёт	1							1
	Всего	34					16	2	16

3.11.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	**Наименование лабораторного занятия**	**Количество часов**
1.2	Основные команды и функциональные клавиши интерфейса командной строки	2
2.2	Расчет IP-сети и IP-подсети, Планирование IP-адресов сети	3
3.2	Агрегация каналов Ethernet и стекирование коммутаторов	3
4.2	Решение NMS и O&M на основе SDN. Решения Huawei NFV	4
5.2	Внедрение сетевой автоматизации. Спецификации кодирования Python	4

Перечень практических занятий

Номер раздела и темы	**Наименование практического занятия**	**Количество часов**
1.1	Основы Huawei VRP	0,4
2.1	Протокол сетевого уровня и IP-адресация	0,4

3.1	Составление и формирование таблицы MAC-адресов	0,4
4.1	Управление сетью. Основы SDN и NFV	0,4
5.1	Сетевое программирование и автоматизация	0,4

3.11.5. Учебно-методическое и информационное обеспечение дисциплины

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей : Пер. с англ. / К. Закер. - СПб. : BHV, 2002. - 988 с.
2. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : Питер, 2014. - 960 с. - (Классика Computer Science).
3. Казаков Ф.А.Администрирование локальных сетей и телекоммуникационных систем: Учеб. пособие / Ф.А. Казаков, Ф.А. Кузьмин. - Томск : СПБ Графикс, 2012. - 157 с.
4. Гуриков, С. Р. Основы алгоритмизации и программирования на Python : учебное пособие / С. Р. Гуриков. - Москва : Инфра-М, 2022. - 343 с. - (Высшее образование: Бакалавриат). - URL: https://znanium.com/catalog/document?id=379975 (дата обращения: 07.09.2021). - ISBN 978-5-16-017142-5.
5. Златопольский, Д. М. Основы программирования на языке Python : учебник / Д. М. Златопольский. - Москва : ДМК Пресс, 2017. - 284 с. - URL: https://e.lanbook.com/book/97359 (дата обращения: 05.08.2021). - ISBN 978-5-97060-552-3
6. Васильев, А. Н. Python на примерах. Практический курс по программированию : учебное пособие / А. Н. Васильев. - 2-е изд. - Санкт-Петербург : Наука и техника, 2017. - 432 с. - URL: https://e.lanbook.com/book/101555 (дата обращения: 05.08.2021). - ISBN 978-5-94387-741-4.

3.11.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: Huawei VRP, Agile Controller-Campus, Python

3.11.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены

выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

3.12. Рабочая программа практики «Сетевое программирование»

3.12.1. Цели и задачи практики

Программа направлена на развитие обучающегося в области программирования и автоматизации сетей. По окончании курса обучающиеся смогут:

- Описывать необходимость и преимущества использования APIs и систем контроля версий для разработки программного обеспечения
- Описывать общие шаги процесса разработки программного обеспечения
- Описывать варианты организации и построения модульного программного обеспечения
- Понимать принципы протокола HTTP и как его использовать в программных интерфейсах
- Применять Representational State Transfer (REST) для интеграции с HTTP-based APIs
- Перечислять ключевые платформы Cisco и их возможности
- Описывать функции программируемости платформ Cisco
- Понимать основные принципы построения сетей
- Понимать принципы взаимодействия приложений с сетью, использовать основные распространенные инструменты для устранения неполадок
- Автоматизировать распространенные сетевые задачи с помощью скриптов Python
- Описывать общие проблемы безопасности, знать типы тестов, использовать контейнеры для локальной разработки
- Использовать различные инструменты автоматизации

3.12.2. Требования к результатам освоения практики

Планируемые результаты освоения программы:

Практика участвует в формировании компетенций: ПК-3 Способен находить и устранять неисправности в сети предприятия и ПК-4 Способен производить модернизацию сети

В результате изучения дисциплины обучающийся должен иметь:

Знания: общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, архитектуры аппаратных, программных и программно-аппаратных средств администрируемых сетевых устройств информационно-коммуникационных систем, протоколов канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем, базовой эталонной модели взаимодействия открытых систем для управления сетевым трафиком, регламентов проведения профилактических работ на администрируемых сетевых устройствах информационно-коммуникационных систем

Умения: производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем, конфигурировать операционные системы сетевых устройств, устанавливать и инициализировать новое программное обеспечение сетевых устройств информационно-коммуникационных систем.

Опыт деятельности: по исправлению ошибок конфигурации сетевых устройств и операционных систем, конфигурированию и эксплуатации сетевых устройств

3.12.3. Учебно-тематический план практики

№	Наименование разделов и тем	Всего, час	Контактная работа, час			ЭО или ДОТ, час			Самостоятельная работа, час
			Лекции	Лабораторные занятия	Практические занятия	Лекции	Лабораторные занятия	Практические занятия	
1.	**Программное обеспечение для управления сетью**	8					4	0,5	3,5
1.1	Общая концепция	1						0,5	0,5
1.2.	Шаблоны и абстракции	7					4		3
2.	**Программный интерфейс приложения**	8					4	0,5	3,5
2.1.	Возможности программирования платформ Cisco	1						0,5	0,5
2.2.	Работа с API Cisco	7					4		3
3.	**Автоматизация работы с сетью**	8					4	0,5	3,5
3.1.	Модели данных	1						0,5	0,5
3.2.	Скрипты автоматизации	7					4		3
4	**Автоматизация рабочего процесса и инфраструктуры**	9					4	0,5	4,5
4.1.	Развертывание приложений	1						0,5	0,5
4.2	Управление и тестирование сети	8					4		4
5.	Промежуточная аттестация: Зачёт	1							1
	Всего	34					16	2	16

3.12.4. Содержание практики

Перечень лабораторных занятий

Номер раздела и темы	Наименование лабораторного занятия	Количество часов
1.2	Разбор форматов данных API с помощью Python. Использование Git для контроля версий. Определение архитектуры программного обеспечения и шаблонов проектирования. Использование шаблонов проектирования одиночка и абстрактная фабрика.	4
2.2	Исследование сообщений протокола HTTP. Использование Postman. Устранение неполадок при получении HTTP Error Response. Взаимодействие с API с использованием Python. Использование Cisco Controller API. Использование Cisco Webex Teams™ Collaboration API	4
3.2	Исследование диаграммы базовой топологии сети. Изучение причин возникновения проблем сетевого подключения в прикладных процессах. Исследование функций протокола Network Configuration Protocol (NETCONF). Использование Cisco Software Development Kit (SDK) и Python для создания скриптов автоматизации	4
4.2	Использование команд Bash для локальной разработки. Создание Unit-тестов Python. Работа с Dockerfile. Использование команд Docker для управления локальной средой разработчика. Построение автоматизированного рабочего процесса	4

Перечень практических занятий

Номер раздела и темы	Наименование практического занятия	Количество часов
1.1	Практика современной разработки программного обеспечения. Введение в сетевые прикладные программные интерфейсы	0,5
2.1	Использование REST-Based API. Возможности программирования платформ Cisco	0,5
3.1	Взаимодействие приложений с сетью. Использование моделей данных YANG	0,5
4.1	Развертывание приложений. Тестирование и защита приложений. Автоматизация инфраструктуры	0,5

3.12.5. Учебно-методическое и информационное обеспечение дисциплины

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей : Пер. с англ. / К. Закер. - СПб. : BHV, 2002. - 988 с.
2. Таненбаум Э. Компьютерные сети: Пер. с англ. / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : Питер, 2014. - 960 с. - (Классика Computer Science).
3. Казаков Ф.А.Администрирование локальных сетей и телекоммуникационных систем: Учеб. пособие / Ф.А. Казаков, Ф.А. Кузьмин. - Томск : СПБ Графикс, 2012. - 157 с.
4. Гуриков, С. Р. Основы алгоритмизации и программирования на Python : учебное пособие / С. Р. Гуриков. - Москва : Инфра-М, 2022. - 343 с. - (Высшее образование: Бакалавриат). - URL: https://znanium.com/catalog/document?id=379975 (дата обращения: 07.09.2021). - ISBN 978-5-16-017142-5.
5. Златопольский, Д. М. Основы программирования на языке Python : учебник / Д. М. Златопольский. - Москва : ДМК Пресс, 2017. - 284 с. - URL: https://e.lanbook.com/book/97359 (дата обращения: 05.08.2021). - ISBN 978-5-97060-552-3
6. Васильев, А. Н. Python на примерах. Практический курс по программированию: учебное пособие / А. Н. Васильев. - 2-е изд. - Санкт-Петербург: Наука и техника, 2017. - 432 с. - URL: https://e.lanbook.com/book/101555 (дата обращения: 05.08.2021). - ISBN 978-5-94387-741-4.

3.12.6. Материально-техническое обеспечение практики

Для доступа к ресурсам практики у обучающегося должен быть компьютер с выходом в интернет, с двусторонней поддержкой видеоконференцсвязи (Zoom/BigBlueButton/Teams и аналогичных), возможность подключения к удалённому рабочему столу, на котором размещено программное обеспечение по практике.

Программное обеспечение по практике: Cisco packet tracer, Cisco Software Development Kit (SDK), Python

3.12.7. Система контроля и оценивания

Оценка качества освоения практики включает текущую и промежуточную аттестацию обучающихся. Оценивается выполнение каждой лабораторной и практической работы. Зачёт по дисциплине выставляется на основании результатов сдачи всех лабораторных и практических работ. Для успешного завершения практики необходимо выполнение всех лабораторных и практических работ при этом не менее 80 % всех лабораторных и не менее 70 % всех практических работ должны быть выполнены в полном объеме с соблюдением необходимой последовательности проведения настроек и оценок параметров оборудования и элементов сети, получены правильные результаты, соблюдены требования правил проектирования сети, составлен отчет, в который правильно внесены все записи, порядок и последовательность выполняемых действий, оценка параметров оборудования и сети, анализ работоспособности выполненных настроек и примененного оборудования, представлены выводы о проделанной работе. Отчётные материалы лабораторных и практических работ загружаются в соответствующие разделы MOODLE.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

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

5. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы переподготовки включает текущую, промежуточную аттестацию в дисциплинах, практиках и итоговую аттестацию обучающихся в виде Экзамена, который принимает комиссия, сформированная из преподавателей и представителей партнеров программы. Допуск до экзамена получают только те обучающиеся, которые успешно освоили все дисциплины и практики и получили по ним зачёты. Экзамен является междисциплинарным и направлен на проверку приобретенных знаний, умений и опыта деятельности. При проверке знаний обучающемуся предлагается пройти тест, сформированный из выборки всех вопросов, изучаемых слушателями в течение всего срока обучения, кроме того, комиссия анализирует успеваемость студентов и вправе задать дополнительные вопросы по дисциплинам, успеваемость по которой ниже средней по всем дисциплинам и практикам программы переподготовки. Для проверки умений и опыта деятельности обучающий должен выполнить контрольные задания на проектирование, настройку и мониторинг сетей и сетевого оборудования, используя программное обеспечение, которое им было изучено при выполнении практических заданий и лабораторных работ.

Конкретные формы и процедуры текущего и промежуточного контроля знаний, умений и опыта деятельности доводятся до сведения обучающихся в течение первого месяца обучения, для итогового контроля не позднее, чем за месяц до окончания обучения.

Разработчики программы:

Зав. каф. ТКС, к.т.н. А.А.Бахтин

Доцент каф. ТКС, к.т.н., доцент А.С. Волков
Доцент каф. ТКС, к.т.н. А.В. Шарамок
Доцент каф. ТКС, к.т.н. А.Г. Тимошенко

Согласовано:

Директор ДРОП Н.Ю. Соколова