МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технологический университет»
(ФГБОУ ВО «КНИТУ»)
ИНСТИТУТ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
(ИДПО КНИТУ)

УТВЕРЖДАЮ
Проректор по УР КНИТУ
_____ Л.Ш. Султанова
«12» _____ 20__ г.

СОГЛАСОВАНО
Директор ИДПО КНИТУ
_____ М.Ф. Галиханов
«___» _____ 20__ г.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы
профессиональной переподготовки

«Компьютерные сети»

Лицензия ФГБОУ ВО «КНИТУ» серия 90Л01, № 0009203, рег. №2165 от 27.05.2016

Программа утверждена на заседании учебно-методической комиссии ИДПО КНИТУ (протокол от 12.09.2022, № 8)

Председатель учебно-методической комиссии _____ В.В. Кондратьев

Казань, 2022 г.

I. Общие положения

1. Дополнительная профессиональная программа (программа профессиональной переподготовки) ИТ-профиля «Компьютерные сети» (далее – Программа) разработана в соответствии с нормами Федерального закона РФ от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», с учетом требований приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», с изменениями, внесенными приказом Минобрнауки России от 15 ноября 2013 г. № 1244 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденный приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499», *приказа Министерства образования и науки РФ от 23 августа 2017 г. N 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ» (указать при необходимости);* паспорта федерального проекта «Развитие кадрового потенциала ИТ-отрасли» национальной программы «Цифровая экономика Российской Федерации»; постановления Правительства Российской Федерации от 13 мая 2021 г. № 729 «О мерах по реализации программы стратегического лидерства «Приоритет-2030» (в редакции постановления Правительства Российской Федерации от 14 марта 2022 г. № 357 «О внесении изменений в постановление Правительства Российской Федерации от 13 мая 2021 г. № 729»); приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 февраля 2022 г. № 143 «Об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» и признании утратившими силу некоторых приказов Министерства цифрового развития, связи и массовых коммуникаций

Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» (далее – приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 143); федерального государственного образовательного стандарта 09.03.01 «Информатика и вычислительная техника» (*Пример: высшего образования по направлению подготовки 09.03.01 Информатика и вычислительная техника (уровень бакалавриата), утвержденного приказом Минобрнауки России от 12 января 2016 г. № 5,* (далее вместе – ФГОС ВО)), а также профессионального стандарта 06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем», (утв. приказом Министерства труда и социальной защиты РФ от 5 октября 2015 г. N 686н). (*Пример: «Программист», утвержденного приказом Министерства труда и социальной защиты РФ от 18 ноября 2013 г. № 679н.)*

2. Профессиональная переподготовка заинтересованных лиц (далее – Слушатели), осуществляемая в соответствии с Программой (далее – Подготовка), имеющей отраслевую направленность[1] «Информационно-коммуникационные технологии», проводится в ФГБОУ ВО «Казанский национальный исследовательский технологический университет (далее – Университет) в соответствии с учебным планом в очной форме обучения[2].

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

[1] Варианты отраслевой направленности: «Городское хозяйство»; «Финансовые услуги»; «Строительство»; «Добывающая промышленность»; «Обрабатывающая промышленность»; «Транспортная инфраструктура»; «Здравоохранение»; «Энергетическая инфраструктура»; «Образование»; «Сельское хозяйство и агропромышленный комплекс»; «Информационно-коммуникационные технологии»; «Искусство и культура»

[2] При реализации Программы допускается использовать сетевую форму обучения с организациями реального сектора экономики субъекта Российской Федерации

коммуникационных систем».

4. Программа регламентирует требования к профессиональной переподготовке в области "06 Связь, информационные и коммуникационные технологии".

Срок освоения Программы составляет 252 часа (*не менее 250 академических часов).*

К освоению Программы в рамках проекта допускаются лица:

- получающие высшее образование по очной (очно-заочной) форме, лица, освоившие основную профессиональную образовательную программу (далее – ОПОП ВО) бакалавриата – в объеме не менее первого курса (бакалавры 2-го курса), ОПОП ВО специалитета – не менее первого и второго курсов (специалисты 3-го курса), обучающиеся по ОПОП ВО, по специальностям и направлениям подготовки ИТ-сферы.

5. Область профессиональной деятельности «"06 Связь, информационные и коммуникационные технологии"».

II. Цель

6. Целью подготовки слушателей по Программе является получение компетенции[3], необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий "06 Связь, информационные и коммуникационные технологии"; приобретение новой квалификации «Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения».

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

[3]Указать целевые группы обучающихся, определенные паспортом Федерального проекта: − обучающиеся по специальностям и направлениям подготовки, не отнесенным к ИТ-сфере, −обучающиеся по специальностям и направлениям подготовки ИТ-сферы (выбрать нужное)

7. Виды профессиональной деятельности, трудовая функция, указанные в профессиональном стандарте по соответствующей должности «Сетевой администратор», представлены в таблице 1:

Таблица 1

Характеристика новой квалификации, связанной с видом профессиональной деятельности и трудовыми функциями в соответствии с профессиональным стандартом «06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»»

Область профессиональной деятельности	Тип задач профессиональной деятельности	Код и наименование профессиональной компетенции	Трудовые действия	Трудовая функция	Обобщенная трудовая функция	Вид профессиональной деятельности
06 Связь, информационные и коммуникационные технологии	*производственно-технологический*	**ПК1-** Администрирует операционные системы (ОС) **ПК2-** Настраивает встроенные средства безопасности операционных систем семейства Linux **ПК3 -** Настраивает сетевое оборудование и средства межсетевого экранирования **ПК4 -** Обеспечивает анализ сетевого	Планирование защиты приложений от несанкционированного доступа Оценка безопасности и защиты приложений от несанкционированного доступа Планирование защиты операционных систем от несанкционированного доступа Оценка защиты операционных систем от несанкционированного доступа	Определение параметров безопасности и защиты программного обеспечения сетевых устройств (D/01.6) Установка специальных средств управления безопасностью администрируемой сети (D/02.6)	Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	Администрирование сетевых устройств информационно-коммуникационной (инфокоммуникационной) системы

		трафика	Параметризация операционных систем дополнительных средств защиты администрируемой сети от несанкционированного доступа Установка специализированных программных средств защиты сетевых устройств администрируемой сети от несанкционированного доступа Установка межсетевых экранов, гибких коммутаторов, средств предотвращения атак виртуальной частной сети Параметризация операционных систем средств удаленного доступа Установка дополнительных программных продуктов для обеспечения безопасности удаленного доступа и их параметризация	Администрирование средств обеспечения безопасности удаленного доступа (операционных систем и специализированных протоколов) (D/03.6)		

			Настройка средств обеспечения безопасности удаленного доступа (операционной системы и специализированных протоколов) Документирование настроек средств обеспечения безопасности удаленного			

Таблица 2

Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере, связанной с уровнем формирования и развития в результате освоения Программы[4] «Компьютерные сети»

Наименование сферы	**Код и наименование профессиональной компетенции**	**Пример инструментов**	**0 — способность не проявляется/ проявляется в степени, недостаточной для отнесения к 1 уровню сформированности компетенции**	**1 — способность проявляется под внешним контролем / при внешней постановке задачи/ обучающийся пользуется готовыми, рекомендованным и продуктами**	**2 — способность проявляется, но обучающийся эпизодически прибегает к экспертной консультации/ самостоятельно подбирает и пользуется готовыми продуктами**	**3 — способность проявляется системно / обучающийся модифицирует способность под определенные задачи / создает новый продукт, обучает других**
Операционные системы	**ПК1- Администрирует операционные системы (ОС)**	Linux и др.	+	+	+	-
	ПК2- Настраивает встроенные средства	Средства администрирования ОС Linux	+	+	+	-

[4] На основании Модели цифровых компетенций, указанной в Приложении 2

	безопасности операционных систем семейства Linux	Средства администрирования Astra Linux				
	ПК3 - Настраивает сетевое оборудование и средства межсетевого экранирования	Iptables, firewald, IPSec, OpenVPN и д.р.	+	+	+	-
	ПК4 - Обеспечивает анализ сетевого трафика	tcpdump, Snort, VipNet-IDS и д.р.	+	+	+	-

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

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

ПК1- Администрирует операционные системы (ОС)

ПК2- Настраивает встроенные средства безопасности операционных систем семейства Linux

ПК3 - Настраивает сетевое оборудование и средства межсетевого экранирования

ПК4 - Обеспечивает анализ сетевого трафика *(Код и наименование профессиональной компетенции Таблица 1)*

В ходе освоения Программы Слушателем совершенствуются следующие профессиональные компетенции:

ПК1- Администрирует операционные системы (ОС)

ПК2- Настраивает встроенные средства безопасности операционных систем семейства Linux

ПК3 - Настраивает сетевое оборудование и средства межсетевого экранирования

ПК4 - Обеспечивает анализ сетевого трафика *(Код и наименование профессиональной компетенции Таблица 2)*

V. Планируемые результаты обучения по ДПП ПП

10. Результатами подготовки слушателей по Программе является получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий "06 Связь, информационные и коммуникационные технологии"; приобретение новой квалификации «Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения».

11. В результате освоения Программы слушатель должен:

Знать:

1) Принципы построения сетей.
2) Сетевые протоколы
3) Маршрутизацию пакетов в компьютерных сетях.
4) Коммутацию.
5) Серверные приложения и операционные системы.
6) Методы защиты компьютерных сетей и серверных приложений.
7) Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети
8) Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети
9) Классификация операционных систем согласно классам безопасности
10) Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных
11) Инструкции по установке администрируемых сетевых устройств
12) Инструкции по эксплуатации администрируемых сетевых устройств
13) Инструкции по установке администрируемого программного обеспечения
14) Инструкции по эксплуатации администрируемого программного обеспечения
15) Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем
16) Модель ISO для управления сетевым трафиком
17) Модели IEEE
18) Защищенные протоколы управления
19) Основные средства криптографии
20) Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе
21) Требования охраны труда при работе с сетевой аппаратурой

администрируемой сети

Уметь:

1) Настраивать сетевое оборудовании.
2) Тестировать работоспособность сети.
3) Настраивать операционные системы и серверные приложения.
4) Настраивать средства защиты сети и серверов
5) Выяснять приемлемые для пользователей параметры работы сети в условиях нормальной (обычной) работы (базовые параметры)
6) Применять аппаратные средства защиты сетевых устройств от несанкционированного доступа
7) Применять программные средства защиты сетевых устройств от несанкционированного доступа
8) Применять программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа
9) Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
10) Настраивать параметры современных программно-аппаратных межсетевых экранов
11) Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
12) Сегментировать элементы администрируемой сети
13) Подключать и настраивать современные межсетевые экраны
14) Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий
15) Работать с контрольно-измерительными аппаратными и программными средствами

Иметь навыки:[5]

1) Настраивать сетевое оборудовании.
2) Мониторинга сети.
3) Устранения ошибок и уязвимостей операционных систем и серверных

[5] Выделяются знания и умения в соответствии с профстандартом, связанные с результатами освоения Программы

приложений.

4) Выявления атак на компьютерные сети

VI. Организационно-педагогические условия реализации ДПП

12. Реализация Программы должна обеспечить получение компетенции, необходимой для выполнения нового вида профессиональной деятельности в области информационных технологий «"06 Связь, информационные и коммуникационные технологии"»; приобретение новой квалификации «Администрирование процесса управления безопасностью сетевых устройств и программного обеспечения».

13. Учебный процесс организуется с применением[6] электронных и дистанционных, инновационных технологий и методик обучения, способных обеспечить получение слушателями знаний, умений и навыков в области[7] «"06 Связь, информационные и коммуникационные технологии"».

14. Реализация Программы обеспечивается научно-педагогическими кадрами Университета, допустимо привлечение к образовательному процессу высококвалифицированных специалистов ИТ-сферы и/или дополнительного профессионального образования в части, касающейся профессиональных компетенций в области администрирования сетей, с обязательным участием представителей профильных организаций-работодателей. Возможно привлечение региональных руководителей цифровой трансформации (отраслевых ведомственных и/или корпоративных) к проведению итоговой аттестации, привлечение работников организаций реального сектора экономики субъектов Российской Федерации.

VII. Учебный план ДПП

[6] При необходимости указать нужное — электронного обучения, дистанционных образовательных технологий

[7] Разрабатывается на основе ФГОС ВО (3++), соответствует разделу 1.11 ФГОС ВО и конкретному профстандарту

15. Объем Программы составляет 252 часов (*не менее 250 академических часов)*

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

Учебный план программы профессиональной переподготовки
«Компьютерные сети»

№ п/п	Наименование раздела (модуля)	Общая трудоемкость (252 часов)	Форма контроля
1.	Компьютерные сети.	90	диф. зачет
2.	Кибербезопасность в компьютерных сетях	90	диф. зачет
3.	Практика	52	диф. зачет
	Промежуточная аттестация	4	-
	Подготовка к итоговой аттестации	14	-
	Итоговая аттестация: в форме демонстрационного экзамена	2	Экзамен
	Итого:	252	

VIII. Календарный учебный график

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

Календарный учебный график программы профессиональной переподготовки «Компьютерные сети»

Календарный учебный график программы профессиональной переподготовки «Компьютерные сети»

№ пп	Наименование раздела (модуля)	Учебные недели																																						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
1.	Компьютерные сети.	+	+	+	+	+	+	+	+	+	+	+	+	+																										
2.	Кибербезопасность в компьютерных сетях														+	+	+	+	+	+	+	+	+	+	+	+	+	+												
4	Практика																			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
5	Промежуточная аттестация													+														+										+		
6	Подготовка к итоговой аттестации																																						+	+
7	Итоговая аттестация: в форме демонстрационного экзамена																																							+

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

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

Рабочая программа разрабатывается Университетом с учетом профессионального стандарта 06.027 «Специалист по администрированию сетевых устройств информационно-коммуникационных систем».

№ п/п	Наименование и краткое содержание раздела(модуля)	Объем, часов
1	**Компьютерные сети.**	**90**
1.1	Основы компьютерных сетей. Стек TCP/IP. Модель OSI. Коммутация пакетов. Управление доступом к портам коммутаторов. Виртуальные локальные сети (VLAN). Операционная система Linux.	14
1.2	Маршрутизация. Прямая маршрутизация. Сетевые интерфейсы. Косвенная маршрутизация. Без классовая маршрутизация. Маска сети. Маршрутизация на Linux. Маршрутизация на Cisco. Служба доменных имен (DNS). Архитектура Internet. Автономные системы. Регистратуры Internet.	10
1.3	Корпоративные информационные системы. ERP–системы, файловые серверы, веб-серверы, почтовые серверы, серверы электронного документооборота и т.д. Автоматическая конфигурация хостов (DHCP). Протоколы прикладного уровня HTTP, FTP, DNS, SMTP, POP3, IMAP4 и т.д.	8
1.4	Методы межсетевого экранирования. Трансляция адресов (NAT). Фильтрация пакетов. Proxy. МЭ на Linux. МЭ на Cisco.	20
1.5	Методы криптографической защиты в сетях. Алгоритмы шифрования. Инфраструктура открытых ключей. Удостоверяющие центры. Виртуальные частные сети (VPN). Протокол IPSec. OpenVPN.	20
1.6	Динамическая маршрутизация. Протоколы RIP, OSPF, BGP. Динамическая маршрутизация на Linux.	16
1.7	Промежуточная аттестация по модулю «Компьютерные сети»	2
2	**Кибербезопасность в компьютерных сетях**	**90**
2.1	Типовые корпоративные компьютерные сети и угрозы в сетях. Методы и средства защиты корпоративных компьютерных сетей.	14
2.2	Изучение конкретной структуры корпоративной сети организации в шаблоне «Киберполигона».	18
2.3	Мониторинг безопасности сетей. Снифферы. Системы обнаружения атак (IDS). Системы предотвращения атак (IPS). Системы	18

	предотвращения утечки информации (DLP). Мониторинг атак смоделированных на «Киберполигоне».	
2.4	Расследование инцидентов в компьютерных сетях. Изучение перехваченного трафика, фалов журналов и т.д. Расследование атак смоделированных на «Киберполигоне».	18
2.5	Выявление и устранение уязвимостей в информационных системах и компьютерных сетях. Выявление и устранение уязвимостей на «Киберполигоне».	20
2.6	Промежуточная аттестация по модулю «Кибербезопасность в компьютерных сетях»	2
3	**Практика**	**52**
4	**Подготовка к итоговой аттестации**	**14**
5	**Итоговая аттестация: в форме демонстрационного экзамена**	**2**
	ИТОГО	**252**

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

№ п/п	Наименование раздела(модуля)	Количество часов		
		аудиторных		самостоятельной работы (выполнение индивидуальных заданий в виртуальной среде)
		Лекции	Лабораторные работы	
1.	**Компьютерные сети.**	**8**	**64**	**18**
2.	**Кибербезопасность в компьютерных сетях**	**8**	**64**	**18**
	Промежуточная аттестация	**4**		
	Практика	**52**		
	Подготовка к итоговой аттестации	**14**		
	Итоговая аттестация: в форме демонстрационного экзамена	**2**		

**указать вид (-ы) запланированной самостоятельной работы*

X. Формы аттестации

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

Итоговая аттестация по Программе проводится в форме демонстрационного экзамена.

22. Лицам, успешно освоившим Программу (в области связи, информационных и коммуникационных технологии", пригодных для практического применения, или навыков использования и освоения цифровых технологий, необходимых для выполнения нового вида профессиональной деятельности) и прошедшим итоговую аттестацию в рамках проекта «Цифровые кафедры», выдается документ о квалификации: диплом о профессиональной переподготовке.

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

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

XI. Оценочные материалы

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

- текущий контроль успеваемости – обеспечивает оценивание хода освоения разделов Программы, проводится в форме приема лабораторных работ;

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

- итоговая аттестация – завершает изучение всей программы.

25. В ходе освоения Программы каждый слушатель выполняет

следующие отчетные работы:

№ п/п	Наименование раздела (модуля)	Задание	Критерии оценки
1.	Компьютерные сети.	Лабораторная работа 1. Настройка сетевых интерфейсов.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум.
		Лабораторная работа 2. Прямая маршрутизация.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 3. Косвенная маршрутизация.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 4. Маска сети.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка

			выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 5. Корпоративные информационные системы.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 6. Виртуальные локальные сети VLAN.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 7. Динамический NAT.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 8. Статический NAT	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 9. Фильтрация пакетов.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов.

			Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 10. Настройка Proxy	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 11. Виртуальные частные сети на IPSec	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 12. Виртуальные частные сети на OpenVPN	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 13. Динамическая маршрутизация	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка

			выставляется, если студент выполнил необходимый минимум
	Промежуточная аттестация	Дифференцированный зачет	Заключается в выполнении контрольной работы по случайной выборки из тем курса Макс. оценка – 22 баллов. Мин. оценка – 8 баллов. Максимальную оценку студент получает, если на все задания выполнены правильно. Минимальная оценка выставляется, если задания выполнены частично.
2.	**Кибербезопасность в компьютерных сетях**	Лабораторная работа 1. Структура киберполигона.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 2. Изучение корпоративной сети предприятия.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 3. Системы мониторинга сетей (IDS).	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 4. Системы мониторинга	Макс. оценка – 6 баллов. Мин. оценка –4 баллов.

		сетей (IDS).	Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 5. Расследование инцидентов по перехваченному трафику в компьютерных сетях.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 6. Расследование инцидентов журналам операционных систем.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 7. Устранение уязвимостей	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 8. Работа в рамках одного из сценариев на киберполигоне.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы.

			Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 9. Работа в рамках одного из сценариев на киберполигоне.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 10. Работа в рамках одного из сценариев на киберполигоне.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 11. Работа в рамках одного из сценариев на киберполигоне.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 12. Работа в рамках одного из сценариев на киберполигоне.	Макс. оценка – 6 баллов. Мин. оценка –4 баллов. Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
		Лабораторная работа 13. Работа в рамках одного из	Макс. оценка – 6 баллов. Мин. оценка –4 баллов.

		сценариев на киберполигоне.	Максимальная оценка выставляется, если студент выполнил полностью все задания лабораторной работы. Минимальная оценка выставляется, если студент выполнил необходимый минимум
	Промежуточная аттестация	Дифференцированный зачет	Заключается в выполнении контрольной работы по случайной выборки из тем курса Макс. оценка – 22 баллов. Мин. оценка – 8 баллов. Максимальную оценку студент получает, если на все задания выполнены правильно. Минимальная оценка выставляется, если задания выполнены частично.

26. Текущий контроль. Перечень примерных заданий
Модуль Компьютерные сети.

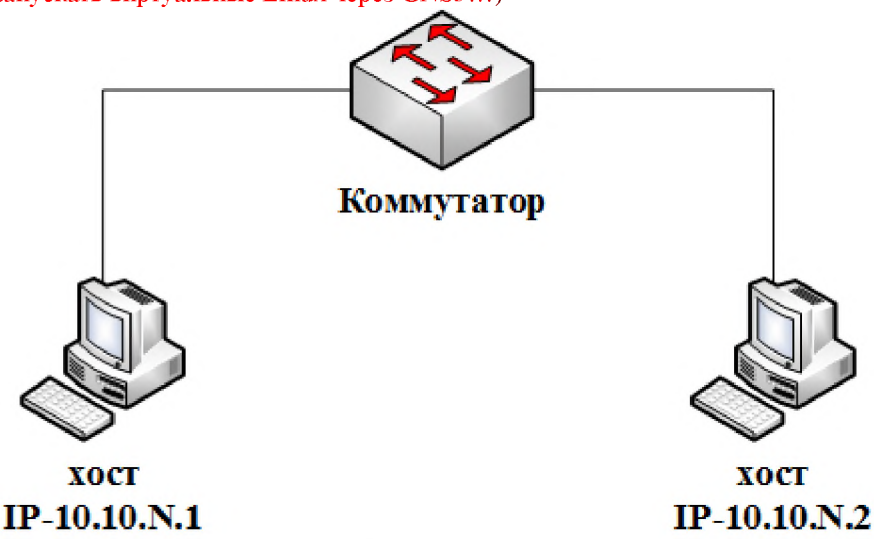
26.1. Тема «Настройка сетевых интерфейсов»

1. создать виртуальную машину
2. в виртуальной машине под Linux настроить сеть для dhcp (в VirtualBox сетевую карту выставить в "сетевой мост")
3. открыть 80 порт
4. запустить http-сервер и проверить из базовой машины через браузер
5. в виртуальной машине добавить еще одну сетевую карту
6. для новой сетевой карты выставить в VirtualBox "сеть NAT"

26.2. Тема «Прямая маршрутизация»

1. настроить в linux сеть 10.10.N.1 для нового интерфейса
   N - последние две цифры из номера зачетки
2. сделать копию виртуальной машины
3. Сгруппируйте свои машины в свою группу (в VirtualBox).

4. собрать сеть в GNS3 (см. рис), 2 хоста на виртуальных Linux соединенные через коммутатор (запускать виртуальные Linux через GNS3!!!)

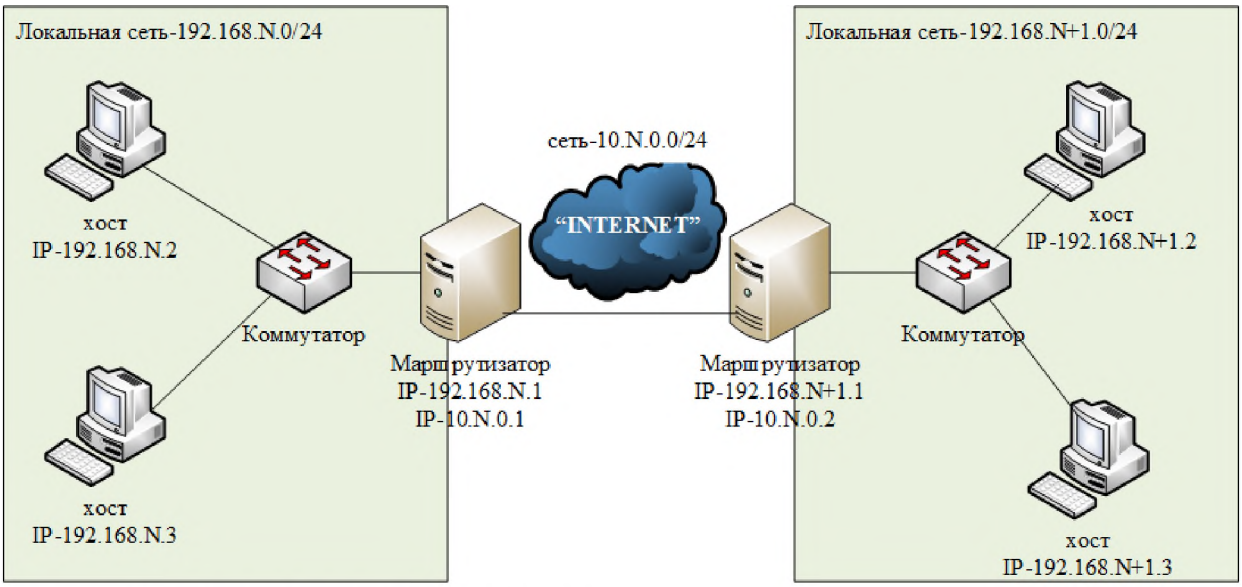


5. проверить работу сети, команды: ping.
6. вывести таблицу маршрутизации, разобрать записи (команда route (с fedora 20 - команда "iproute"))
7. сделать статические записи в ARP таблицы для всех интерфейсов (команда arp (с fedora 20 - команда "ipneighbour"))
8. настроить MTU=12N
   N - последние две цифры из номера зачетки

проверить прохождение пакетов разных размеров с помощью ping

26.3. Тема «Косвенная маршрутизация»

1. соберите схему сети
   одна сеть -192.168.N.0/24 (назвать "сеть NAT" - 1 локальная сеть)
   вторая - 10.N.0.0/24 (назвать "сеть NAT" - глобальная глобальная)
   третья - 192.168.N+1.0/24 (назвать "сеть NAT" - 2 локальная сеть)
   N - "последние две цифры из номера зачетки"



2. настроить прямую маршрутизацию в локальных сетях
3. проверить с помощью ping
4. настроить косвенную маршрутизацию на всех маршрутизаторах и хостах
5. проверить с помощью traceroute
6. проверить прохождение пакетов разных размеров с помощью traceroute и ping (ваше MTU=12N, N - последние две цифры из номера зачетки)
7. Разобрать теорию: Коммутация каналов. Коммутация пакетов. Маршрутизация.

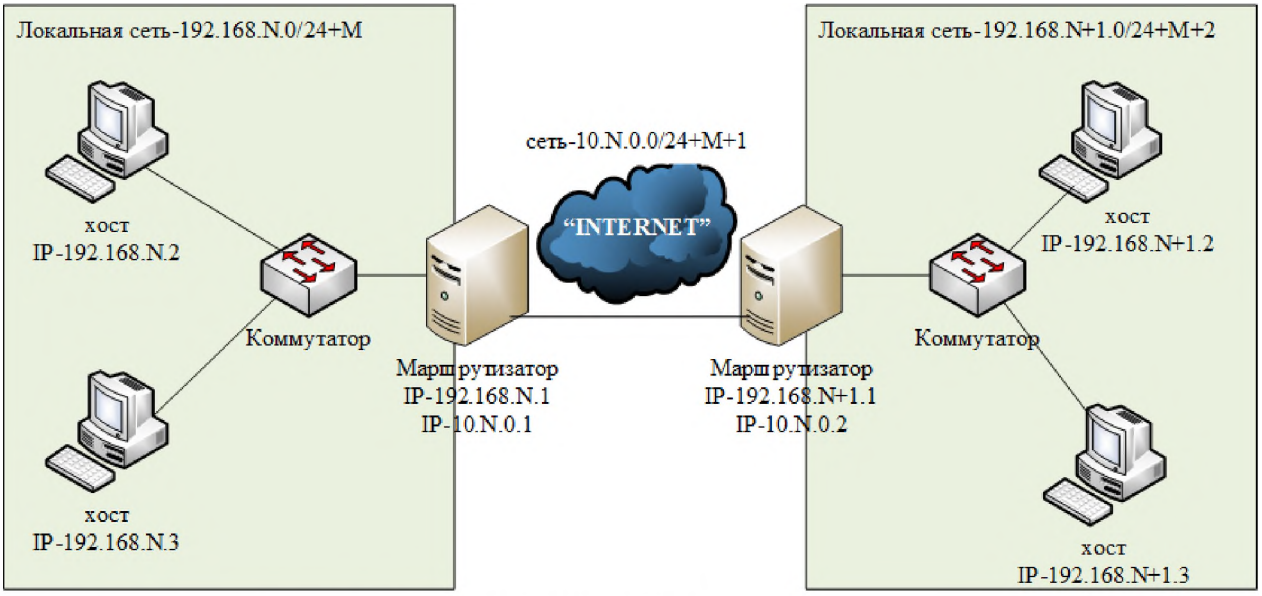
8. Пройти учебный тест по 2 лекции (набрать не менее 60%)

При сдаче:

1. показать пройденный тест по 2 лекции (не менее 60%)
2. показать настройки сети
3. показать настройки маршрутизации
4. продемонстрировать маршрут по цепи
5. показать прохождение пакетов с помощью tcpdump

26.4. Тема «Маска сети»

1. построить сеть по схеме
   вместо сети класса "C", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
2. проверить прохождение пакетов разных размеров с помощью traceroute и ping (ваше MTU=12N, N - последние две цифры из номера зачетки)



3. Проверить косвенную маршрутизацию с помощью traceroute
4. Разобрать теорию: ARP-протокол (для чего и принцип работы).
5. Пройти учебный тест по 3 лекции (набрать не менее 60%)

При сдаче:

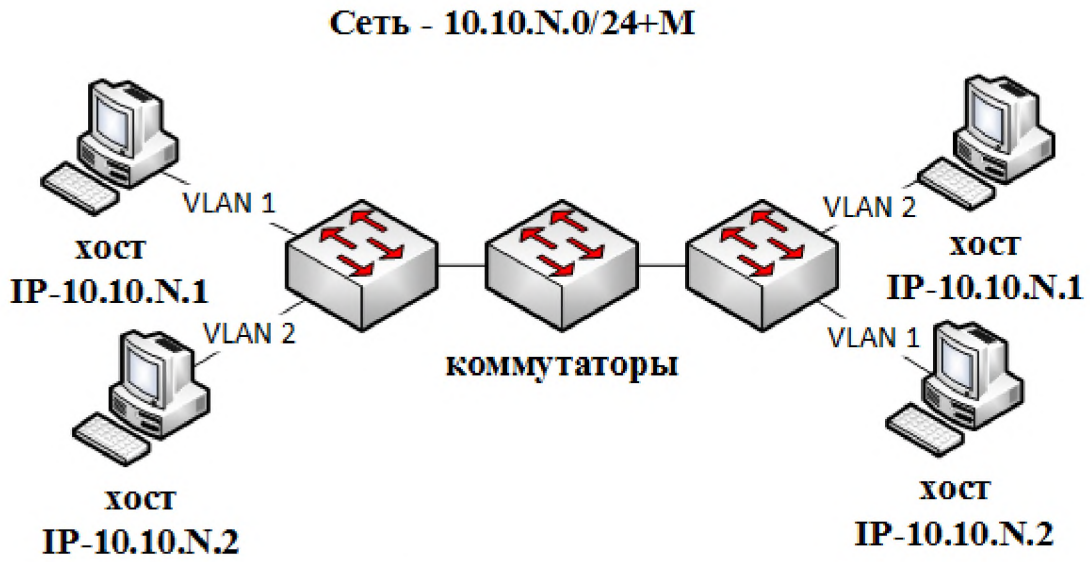
1. показать пройденный тест по 3 лекции (не менее 60%)
2. показать и пояснить расчет маски
3. показать настройки сети
4. настроить прямую маршрутизацию между сетями
5. соединить все виртуальные машины в одну цепь с помощью косвенной маршрутизации
6. показать прохождение пакетов с помощью tcpdump

26.5. Тема «Корпоративные информационные системы»

1. Настроить в своей сети, по выбору одну из корпоративных информационных систем (ERP–системы, файловые серверы, веб-серверы, почтовые серверы, серверы электронного документооборота и т.д.).
2. Продемонстрировать работу.

26.6. Тема «Виртуальные локальные сети VLAN»

1. Построить сеть по схеме
   сеть 10.10.N.0 /24+M значащих бит
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   N - последние 2 цифры в зачетке.
2. Настройте VLAN таким образом:
   - хосты 1 и 4 в VLAN №1
   - хост 2 и 3 в VLAN №2
   т.е. VLAN №1 и №2 не должны взаимодействовать между собой.



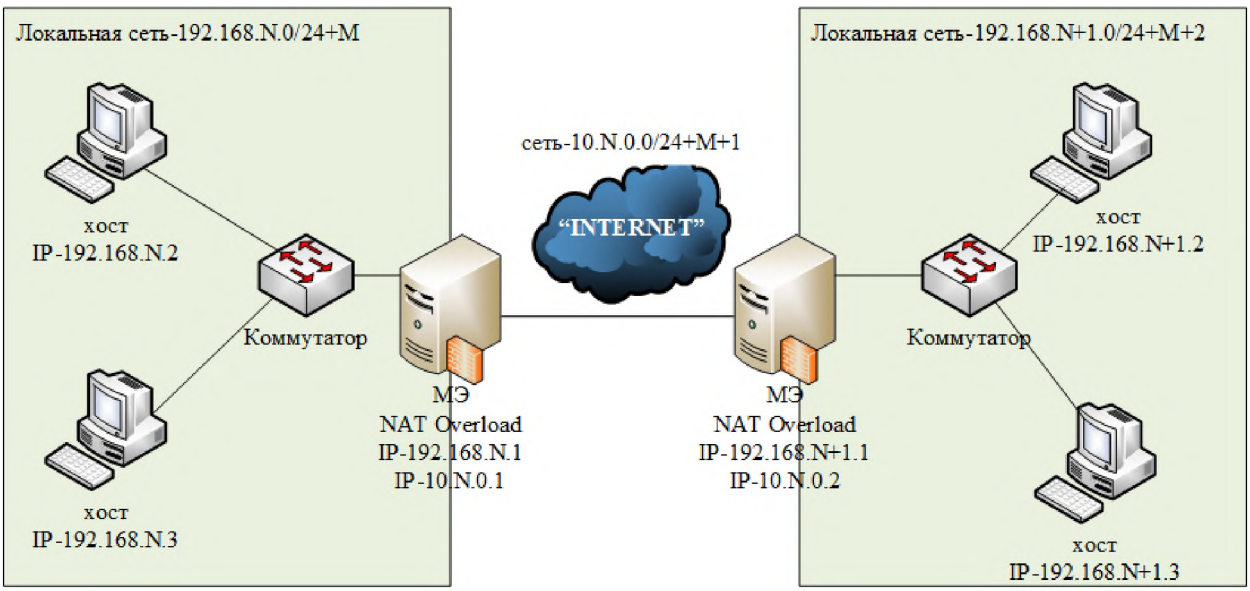
3. Разобрать теорию: VLAN (для чего и принцип работы).
4. Пройти учебный тест по 5 лекции (набрать не менее 60%)

При сдаче:

1. Показать пройденный тест (не менее 60%)
2. Продемонстрировать работу VLANs

26.7. Тема «Динамический NAT»

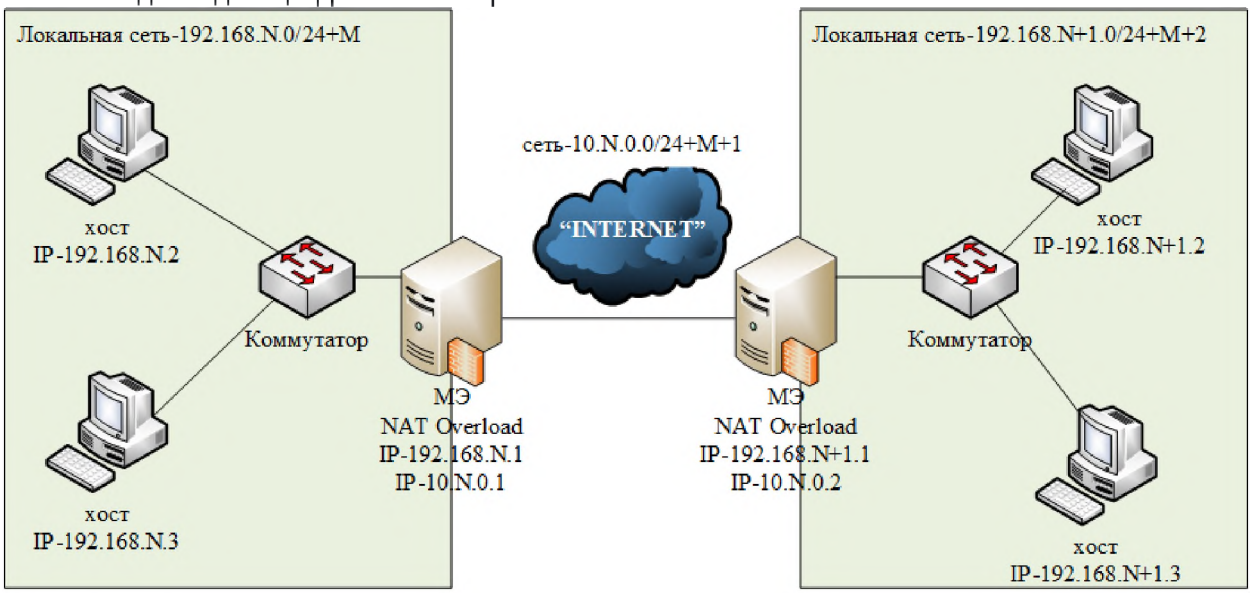
1. построить сеть по схеме
   вместо сети класса "С", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
   N - последние две цифры из номера зачетки



2. на шлюзах разрешить форвардинг пакетов между интерфейсами
3. удалить firewalld
4. отключить selinux
5. дать имена для всех IP и прописать в файле host
6. на маршрутизаторах настроить динамический NAT-Overload используя iptables
   создать запускаемый файл, в нем 3 строки
   1) очистка правил iptables
   2) правило для исходящий пакетов
   3) правило для входящих пакетов
7. на хостах поднять httpd или ssh для диагностики

26.8. Тема «Статический NAT»

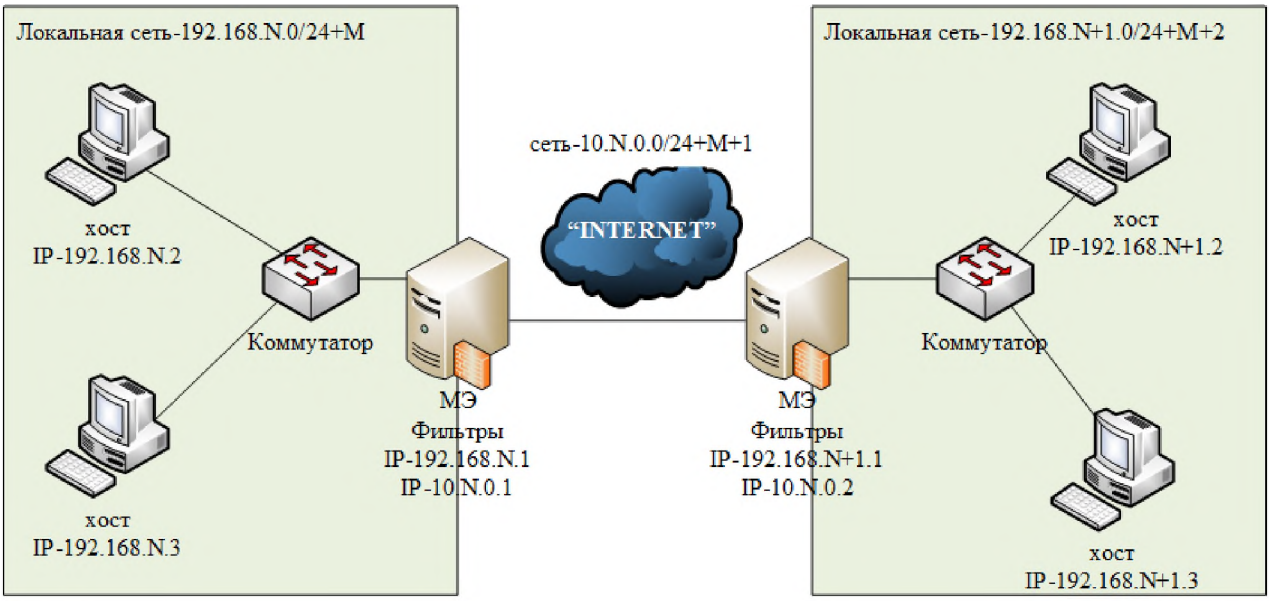
1. построить сеть по схеме **(скриншот сети)**
   вместо сети класса "C", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
   N - последние две цифры из номера зачетки



2. на маршрутизаторах настроить статический NAT используя iptables
3. создать запускаемый файл, в нем 3 строки
   1) очистка правил iptables
   2) правило для исходящий пакетов
   3) правило для входящих пакетов
4. на хостах поднять httpd или ssh для диагностики
5. Показать трассировки маршрутов.
6. С помощью ping, traceroute и tcpdump произвести диагностику преобразования адресов.

26.9. Тема «Фильтрация пакетов»

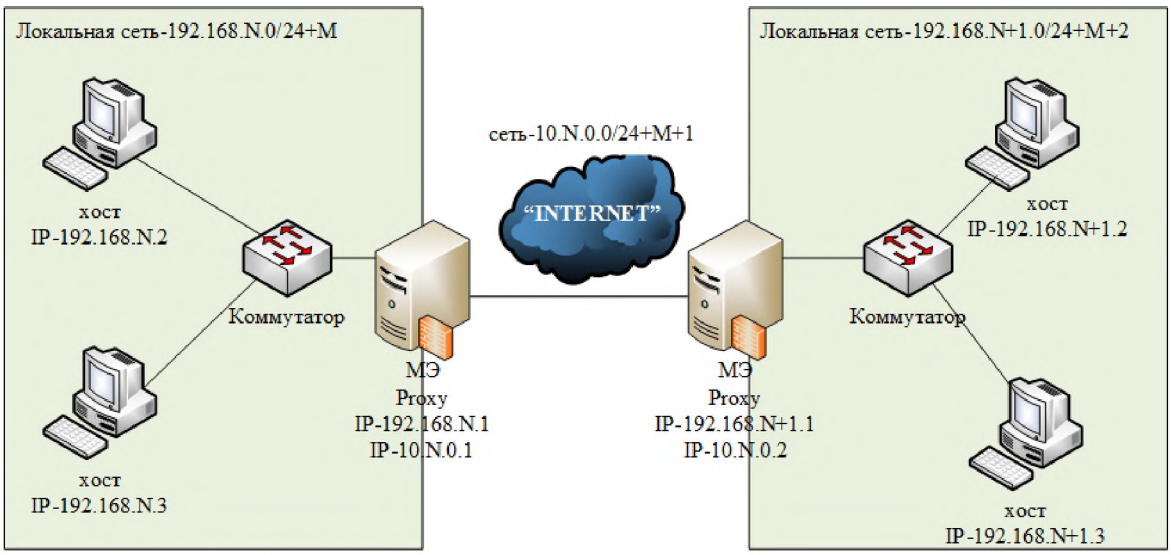
1. построить сеть по схеме
   вместо сети класса "С", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
   N - последние две цифры из номера зачетки



2. на маршрутизаторах настроить фильтры IP пакетов (политика безопасности: в 1- локальной сети - "все запрещено", во 2- локальной сети - "все разрешено")
   - в 1-й ЛК разрешить прохождение пакетов хоста 192.168.N.N
   - в 2-й ЛК блокировать хост с адресом 192.168.N+1.N

26.10. Тема «Настройка Proxy»

1. построить сеть по схеме
   вместо сети класса "С", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
   N - последние две цифры из номера зачетки

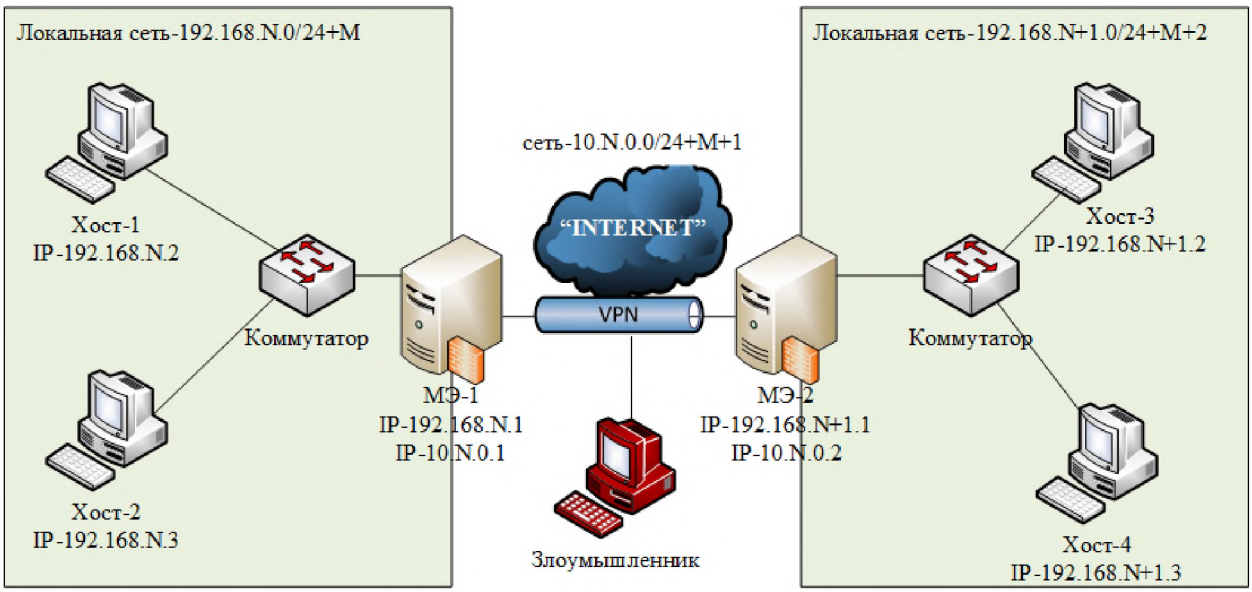


2. установить proxy-сервер Squid

3. настроить проброс через прокси HTTP пакетов (не прозрачный, not *transparent*)
4. настроить на клиентских машинах proxy в браузерах

26.11. Тема «Виртуальные частные сети на IPSec»

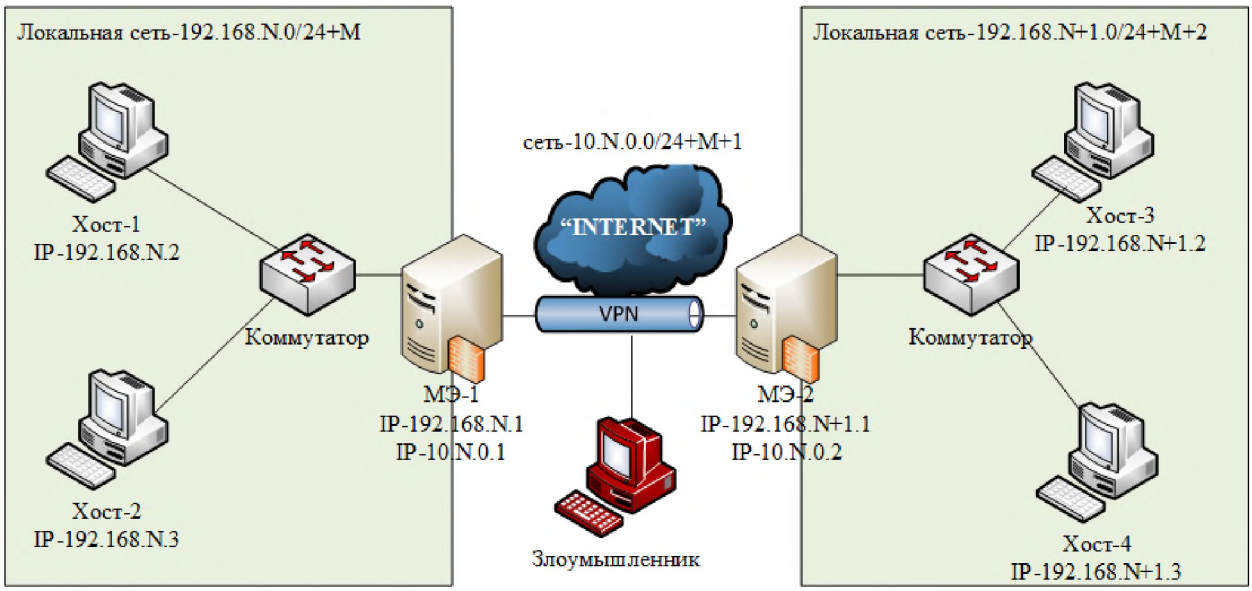
1. построить сеть по схеме
   вместо сети класса "C", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
   N - последние две цифры из номера зачетки



2. на МЭ настроить VPN из одной ЛС во вторую ЛС на IPsec
   - сети 192.168.N.0/24+M и 192.168.N+1.0/24+M+2 должны видеть друг друга
   - алгоритм шифрования - четные зачетки "3des", нечетные зачетки "aes"
   - алгоритм аутентификации - четные зачетки "hmac_md5", нечетные зачетки "hmac_sha512"
   - алгоритм сжатия - deflate
3. добавьте в сеть "злоумышленника" между маршрутизаторами (в настройках сети включить "Неразборчивый режим" (Promiscuous Mode)), посмотрите с помощью tcpdump передаваемый трафик.

26.12. Тема «Виртуальные частные сети на OpenVPN»

1. построить сеть по схеме **(скриншот сети)**
   вместо сети класса "C", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.
   вторая сеть /24+M+1 значащих бит
   третья сеть /24+M+2 значащих бит
   N - последние две цифры из номера зачетки



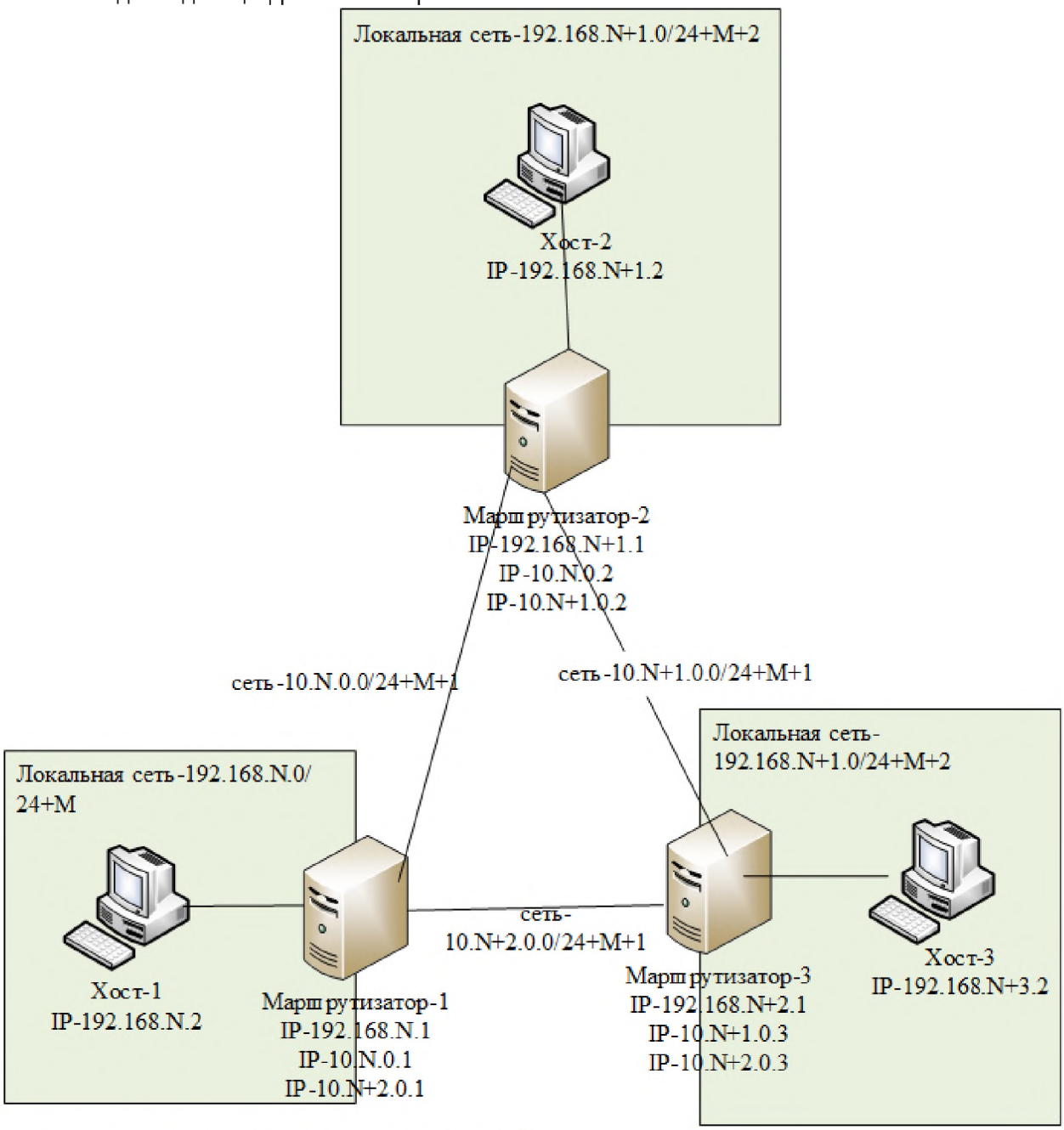
2. на МЭ настроить VPN из одной ЛС во вторую ЛС на OpenVPN
   - сети 192.168.N.0/2M и 192.168.N+1.0/2M должны видеть друг друга

3. добавьте в сеть "злоумышленника" между маршрутизаторами (в настройках сети включить "Неразборчивый режим" (Promiscuous Mode)), посмотрите с помощью tcpdump передаваемый трафик (показать содержимое пакетов).

26.13. Тема «Динамическая маршрутизация»

1. построить сеть по схеме
   вместо сети класса "C", настроить сеть на конкретное количество хостов, значащих бит /24+M
   M - последняя цифра в зачетке деленная на 2, и округленная до целого в меньшую сторону.

N - последние две цифры из номера зачетки



2. на маршрутизаторах настроить протокол RIP
3. имитировать разрывы сетей, наблюдая за перестроением маршрутов
4. запишите время перестроения для каждой сети

Модуль Кибербезопасность в компьютерных сетях.

26.14. Тема «Структура киберполигона»

1. Ознакомится с архитектурой киберполигона.
2. Ознакомится с основными инструментами.

26.15. Тема «Изучение корпоративной сети предприятия»

1. Изучить корпоративную сеть предприятия одного из сценариев (сценарии

расписаны в методических указаниях к киберполигону).

26.16. Тема «Системы мониторинга сетей (IDS)»

1. Ознакомится с системой обнаружения атак ViPNet-IDS.

26.17. Тема «Системы мониторинга сетей (IDS)»

1. Ознакомится с системой обнаружения атак Security Onion.

26.18. Тема «Расследование инцидентов по перехваченному трафику в компьютерных сетях»

1. С помощью систем обнаружения атак, анализируя трафик выявить атаки (сценарии расписаны в методических указаниях к киберполигону).
2. Заполнить карточку инцидента для каждой атаки.

26.19. Тема «Расследование инцидентов журналам операционных систем»

1. Выявить следы обнаруженных атак в предыдущей лабораторной в журналах операционных систем (сценарии расписаны в методических указаниях к киберполигону).
2. Дополнить карточки инцидентов дополнительной информацией.

26.20. Тема «Устранение уязвимостей»

1. Найти уязвимости по обнаруженным атакам (сценарии расписаны в методических указаниях к киберполигону).
2. Устранить уязвимости.

26.21. Тема «Работа в рамках одного из сценариев на киберполигоне»

1. Проведение киберучения по одному из сценария.

Защита базы данных предприятия

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам. Обнаружив и проэксплуатировав уязвимость на нем, нарушитель получает доступ к серверу, который помимо основной информационной задачи предоставляет пользователям Компании инструмент для генерации отчетов. С помощью этого вектора нарушитель пробует получить доступ на рабочие машины сотрудников. Главная цель – сделать дамп корпоративной базы данных.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

26.22. Тема «Работа в рамках одного из сценариев на киберполигоне»

1. Проведение киберучения по одному из сценария.

Защита контроллера домена предприятия

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам компании. Обнаружив несколько уязвимостей на внешнем периметре и закрепившись на одном из серверов, Злоумышленник проводит разведку корпоративной сети с целью захватить контроллер домена.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

Злоумышленник обладает опытом проведения почтовых фишинговых рассылок.

26.23. Тема «Работа в рамках одного из сценариев на киберполигоне»

1. Проведение киберучения по одному из сценария.

Защита данных файлового сервера

Внешний злоумышленник находит в интернете сайт Компании и решает провести атаку на него с целью получения доступа к внутренним ресурсам. На сайте был обнаружен раздел для входа в личный кабинет, который не содержит защитных механизмов от атаки перебора учетных данных. Нарушитель смог успешно подобрать параметры входа для одного из пользователей.

Использование одинаковых паролей для различных сервисов позволило нарушителю получить доступ к почтовому ящику сотрудника и далее успешно подключиться к его рабочей станции, с которой он атаковал внутренний файловый сервис с помощью уязвимости в windows-реализации SMB-протокола.

Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

26.24. Тема «Работа в рамках одного из сценариев на киберполигоне»

1. Проведение киберучения по одному из сценария.

Защита данных сегмента АСУ ТП

Внешний злоумышленник находит в интернете веб-сервер Компании и решает провести атаку на него с целью получения доступа в сегмент АСУ ТП.

На сервере была обнаружена конфигурационная уязвимость, которая предоставила нарушителю дополнительную техническую информацию. Получив сведения о схеме пересылки почтовых сообщений, злоумышленник формирует письмо со специальным вложением. Один из сотрудников открывает файл и просматривает его до страницы со сгенерированным содержимым, тем самым предоставив нарушителю доступ к своему компьютеру. Злоумышленник далее успешно развивает атаку в сторону сегмента АСУ ТП.
Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

26.25. Тема «Работа в рамках одного из сценариев на киберполигоне»

1. Проведение киберучения по одному из сценария.

Защита научно-технической информации предприятия
Внутренняя служба безопасности не смогла обнаружить в новом сотрудники специально подготовленного агента, который устроился в компанию для получения сведений, касающихся разработки новых насосных станций.
Внутренний нарушитель проводит ряд успешных атак как на внутренних сотрудников компании, так и на сервера ЦОД. В результате он смог подключиться к внутренней базе данных и получить значения технических параметров работы новых насосных станций.
Квалификация нарушителя высокая. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

26.26. Тема «Работа в рамках одного из сценариев на киберполигоне»

1. Проведение киберучения по одному из сценария.

Защита корпоративного портала от внутреннего нарушителя
В Компанию устроился сотрудник, который достаточно качественно выполняет свои обязанности. Однако, в свободное время он увлекается пентестом и решает практические задачи на платформе Hack The Box.
При закрытии достаточно успешного проекта у сотрудника возник конфликт со своим руководителем по размеру выданной премии. Сотрудник решает провести атаку на внутренний портал организации, чтобы в нелицеприятном свете показать своего руководителя.
Нарушитель проводит ряд успешных атак на внутренние сервера Компании. В результате он смог получить административный доступ к корпоративному порталу, что дало ему возможность размещать любую информацию.
Квалификация нарушителя средняя. Он умеет использовать инструментарий для проведения атак, а также знает техники постэксплуатации.

27. Промежуточная аттестация. Перечень примерных заданий
Модуль Компьютерные сети
27.1. Тема «Все темы модуля»

На итоговой контрольной лабораторной выпадает одна из лабораторных работ из выполненных, но со случайными параметрами.

Модуль Кибербезопасность в компьютерных сетях.
27.2. Тема «Все темы модуля»

На итоговой контрольной лабораторной выпадает один из сценариев на киберполигоне, необходимо выявить атаки и устранить уязвимости.

28. Итоговая аттестация. Перечень примерных заданий
Модуль по всем модулям
26.1. По всем тема

Проводится в виде демонстрационного экзамена на киберполигоне, по одному из сценариев.

XII. Материально-техническое и учебно-методическое обеспечение Программы

1. Киберполигон “Ampire” (с методическими материалами)
2. Компьютерный класс
3. УМК компании **“**ИнфоТеКС**”**
4. По от «Фактор-ТС»
5. Типовой комплект учебного оборудования "Глобальные компьютерные сети" (с методичками по лабораторным работам)
6. Типовой комплект учебного оборудования "Корпоративные компьютерные сети" (с методичками по лабораторным работам)
7. Типовой комплект учебного оборудования «Телекоммуникационные линии связи» ТЛС-02 (с методичками по лабораторным работам)
8. Программное обеспечение для виртуализации GNS3, VirtualBox.
9. Операционные системы Linux.

XIII. Список литературы

1. **Таненбаум, Эндрю.** Компьютерные сети (любое издание).
2. **Олифер, Виктор Григорьевич.** Компьютерные сети: принципы, технологии, протоколы (любое издание).

3. **Э. Таненбаум,** Современные операционные системы. (любое издание)
4. **Н. А. Олифер, В. Г. Олифер,** Сетевые операционные системы: Учебник для вузов. (любое издание)