Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 01.09.2022 15:08
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
«Информационные технологии»
_____/Д.Г.Демидов/
«16» мая 2022

Рабочая программа дисциплины

«Сети и системы передачи информации»

Направление подготовки/специальность
09.03.01 Информатика и вычислительная техника

Профиль/специализация
«Системная и программная инженерия»

Квалификация
Бакалавр

Формы обучения
очная

Москва, 2022 г.

Разработчик(и):

к.т.н., доцент / А.В. Карпов /
Старший преподаватель / П.В. Максимов /

Согласовано:
Заведующий кафедрой «Инфокогнитивные технологии»,
к.т.н., доцент / Е.А. Пухова /

Руководитель образовательной программы /А.Ю.Гневшев/

1. Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Сети и системы передачи информации» относится:

• формирование комплексных знаний о принципах организации, функционирования и использования компьютерных сетей различного масштаба, возможностей их реализации на основе базовых технологий и стандартов;

• формирование умений и навыков по построению современных сетевых топологий и систем связи, использованию перспективных технологий, стандартов и протоколов передачи данных;

• закрепление получаемых в семестре знаний и навыков на практике;

• формирование взаимосвязей, получаемых в семестре знаний и навыков с изученными ранее и изучаемых параллельно с данной дисциплиной;

• подготовка студентов к деятельности в соответствии с квалификационной характеристикой бакалавра.

К **основным задачам** дисциплины «Сети и системы передачи информации» относятся:

• овладение навыками и приемами использования технических и программных компонентов сетей и систем передачи информации, сетевых протоколов и алгоритмов передачи информации для достижения профессиональных целей;

• изучение и освоение теоретического материала, как в процессе контактной, так и в ходе самостоятельной работы;

• выполнение предоставленных практических заданий различных форм, как в процессе контактной, так и в ходе самостоятельной работы;

• самостоятельная работа над тематикой дисциплины для формирования компетенций основной образовательной программы (далее, ООП).

В результате освоения дисциплины у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций.

Код и наименование компетенции	**Индикаторы планируемых результатов обучения по дисциплине**
ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5.1. Знать: основы системного администрирования. ОПК-5.2. Уметь: выполнять подключение, установку и проверку аппаратных, программно-аппаратных и программных средств. ОПК-5.3. Владеть: методами установки системного и прикладного программного обеспечения.
ОПК-7. Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть: способами проверки работоспособности программно-аппаратных комплексов.
ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-8.1. Знать: операционные системы и оболочки.

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Сети и системы передачи информации» относится к числу учебных дисциплин обязательной части Б1.1 учебного плана основной профессиональной образовательной программы.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами:

- Б1.1.9 Основы информационно-коммуникационных технологий.
- Б1.1.10 Организация ЭВМ и вычислительных систем
- Б1.1.15 Основы сетевых технологий

3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 академических часов, из них 72 часа – самостоятельная работа студентов).

Разделы дисциплины изучаются на втором курсе в третьем семестре, форма промежуточной аттестации - экзамен.

3.1. Виды учебной работы и трудоемкость для очной формы обучения)

№ п/п	Вид учебной работы	Количество часов	Семестры	
			3	
1	Аудиторные занятия	72	72	
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	72	
2	Самостоятельная работа	72	72	
3	Промежуточная аттестация:			
	Курсовой проект			
	Экзамен		экзамен	
	Итого:	144	144	

3.2. Тематический план изучения дисциплины для очной формы обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
			Аудиторная работа				
		Всего	Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	Самостоятельная работа
1	Тема 1 Современные угрозы сетевой безопасности						9
2	Тема 2 Обеспечение безопасности сетевых устройств				5		9
3	Тема 3 Аутентификация, авторизация и учет				6		9
4	Тема 4 Внедрение технологий межсетевого экрана				16		9
5	Тема 5 Внедрение системы предотвращения вторжений						9
6	Тема 6 Обеспечение безопасности локальной сети (LAN)				20		9
7	Тема 7 Криптографические системы				15		9
8	Тема 8 Управление безопасной сетью				10		9
	Всего часов по дисциплине на втором курсе	144			72		72

3.3.Содержание дисциплины

Тема 1 Современные угрозы сетевой безопасности

1.2 Сетевые угрозы

1.2.2 Инструменты хакера

• Атака с модификацией данных

• Атака спуфинга IP-адресов

1.2.4 Распространенные сетевые атаки

1.3 Нейтрализация угроз8

1.3.4 Устранение типичных сетевых атак

• Способы нейтрализации атак для получения доступа

1.3.5 Структура защиты сетевой платформы Cisco

Тема 2 Обеспечение безопасности сетевых устройств

2.1 Защита доступа к устройствам

2.1.1 Защита граничного маршрутизатора

2.1.2 Конфигурирование безопасного административного доступа

• Рекомендации по надежным паролям

• Примеры ненадежных паролей

• Примеры надежных паролей

2.1.3 Конфигурирование усовершенствованных функций

2.1.4 Конфигурирование SSH

2.2 Назначение административных ролей

2.2.1 16 уровней привилегий

• Уровни привилегий

2.2.2 Конфигурирование CLI на основе ролей

2.3 Мониторинг устройств и управление ими

2.3.1 Защита файлов конфигурации и образа Cisco IOS

• Сведения об устойчивой конфигурации Cisco IOS

2.3.2 Защита управления и отчетности

• Особенности внеполосного (OOB) управления

2.3.3 Использование системного журнала (Syslog) для защиты сети

2.3.4 Использование протокола SNMP для защиты сети

2.3.5 Использование NTP

2.4 Использование автоматических функций обеспечения безопасности

2.4.1 Выполнение аудита безопасности

2.5 Защита плоскости управления

2.5.1 Аутентификация протокола маршрутизации

2.5.2 Ограничение плоскости управления

Лабораторная работа №1 Настройка операций Syslog, NTP и SSH на маршрутизаторах Cisco

Тема 3 Аутентификация, авторизация и учет

3.1 Назначение AAA

3.1.1 Обзор AAA

3.1.2 Характеристики AAA

• Типы учетной информации

3.2 Локальная аутентификация AAA

3.2.1 Настройка локальной аутентификации AAA с помощью CLI

3.2.2 Устранение ошибок локальной аутентификации AAA

3.3 Серверное решение AAA

3.3.1 Характеристики серверного решения AAA

3.3.2 Коммуникационные протоколы серверного AAA

• Сравнение TACACS+ и RADIUS

3.4 Серверная аутентификация AAA

3.4.1 Настройка аутентификации на сервере

3.4.2 Исправление ошибок серверной аутентификации AAA

3.5 Серверная авторизация и учет AAA
3.5.1 Настройка серверной авторизации AAA
3.5.2 Настройка серверного учета AAA
3.5.3 Аутентификация 802.1X
Лабораторная работа №14 Настройка аутентификации AAA на маршрутизаторах Cisco

Тема 4 Внедрение технологий межсетевого экрана

4.1 Списки контроля доступа (ACL)
4.1.1 Настройка стандартных и расширенных списков контроля доступа
4.1.2 Нейтрализация атак с помощью списков ACL
4.1.3 ACL-списки IPv6
4.2 Технологии межсетевого экрана
4.2.1 Защита сетей с помощью межсетевых экранов
4.2.2 Типы межсетевых экранов
4.2.3 Классический межсетевой экран
4.2.4 Межсетевые экраны в дизайне сети
• Практические рекомендации для межсетевого экрана
Лабораторная работа №6 Настройка расширенных списков контроля доступа (ACL)
Лабораторная работа №7 Настройка списков контроля доступа (ACL) для IPv6
Лабораторная работа №8 Устранение неполадок в работе стандартных списков контроля доступа для IPv4

Тема 5 Внедрение системы предотвращения вторжений

5.1 Технологии IPS
5.1.1 IDS и характеристики IPS
5.1.2 Варианты сетевой реализации IPS
5.1.3 Анализатор коммутируемых портов Cisco
5.2 Сигнатуры IPS
5.2.1 Характеристики сигнатур для IPS-систем
5.2.2 Сигналы тревоги сигнатур IPS
5.2.3 Действия сигнатур IPS
• Сводка категорий действий
• Сброс подключения и блокировка действия
5.2.4 IPS для управления и мониторинга
• Факторы, которые необходимо учесть при планировании и мониторинге IPS
• Способ управления

Тема 6 Обеспечение безопасности локальной сети (LAN)

6.1 Безопасность оконечных устройств
6.1.1 Введение в безопасность оконечных устройств
• Защита оконечных устройств
• Хостовая реализация IPS
6.2 Факторы, которые необходимо учитывать при обеспечении безопасности на 2-м уровне
6.2.1 Угрозы безопасности на 2-м уровне
• Атаки на DHCP
• Атаки на ARP
• Атаки спуфинга адресов
• Атаки на STP
6.2.2 Атаки на таблицу CAM
6.2.3 Нейтрализация атак на таблицы CAM
• Режимы нарушения защиты
• Защита
• Ограничение
• Завершение работы
6.2.5 Нейтрализация атак DHCP
6.2.8 Протокол связующего дерева

• Стоимость портов по умолчанию STP

6.2.9 Нейтрализация атак STP

Лабораторная работа №2 Исследование методов реализации сети VLAN

Лабораторная работа №3 Настройка сетей VLAN

Лабораторная работа №4 Настройка магистральных каналов

Лабораторная работа №11 Проверка и отладка настроек NAT

Тема 7 Криптографические системы

7.1 Криптографические сервисы

7.1.1 Защита обмена данными

7.1.4 Криптология

7.2 Основные вопросы целостности и аутентификации

7.2.1 Криптографические хеш-функции

7.2.2 Целостность с алгоритмами MD5, SHA-1 и SHA-2

7.2.3 Аутентификация с помощью алгоритма HMAC

Лабораторная работа №5 Настройка стандартных именованных списков контроля доступа IPv4

Лабораторная работа №9 Межсетевые экраны на сервере и списки контроля доступа на маршрутизаторе

Лабораторная работа №10 Обеспечение безопасности VLAN на 2-м уровне

Тема 8 Управление безопасной сетью

8.1 Тестирование безопасности сети

8.1.1 Методики тестирования безопасности сети

Тестирование и оценка системы безопасности (ST&E)

8.1.2 Инструменты тестирования безопасности сети

Лабораторная работа №12 Отказоустойчивость маршрутизаторов и коммутаторов

Лабораторная работа №13 Резервирование маршрутизаторов и коммутаторов

Методика преподавания дисциплины «Сети и системы передачи информации» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков у обучающихся:

• выполнение лабораторных работ в лабораториях вуза;

• индивидуальные и групповые консультации студентов преподавателем;

• посещение профильных конференций и работа на мастер-классах экспертов и специалистов в веб-технологиях, веб-разработке, Интернет-маркетинге и других профессиональных областях.

Самостоятельная внеаудиторная работа студентов состоит из подготовки к выполнению и защите лабораторных работ, а также подготовки к промежуточной аттестации во время экзаменационной сессии.

4. Учебно-методическое и информационное обеспечение

4.1.Нормативные документы и ГОСТы

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

2. Приказ Минобрнауки России от 19.09.2017 N 929 (ред. от 08.02.2021) «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника» (Зарегистрировано в Минюсте России 10 октября 2017 г. N 48489).

3. Академический учебный план Направление подготовки: 09.03.01 Информатика и вычислительная техника Профиль: Кибербезопасность автоматизированных систем Форма обучения: очная.

4. Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет» (Утверждено приказом Московского Политеха от 01.12.2022 № 1375ОД).

4.2. Основная литература

1. Сети и телекоммуникации: учебник и практикум для вузов / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 464 с. — (Высшее образование). — ISBN 978-5-534-17315-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532855

2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях: учебник и практикум для вузов / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 423 с. — (Высшее образование). — ISBN 978-5-534-16546-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531273

4.3. Электронные образовательные ресурсы

1. https://online.mospolytech.ru/course/view.php?id=13237

4.4. Дополнительная литература

1. Трофимов, В. В. Глобальные и локальные сети: учебник для вузов / В. В. Трофимов, М. И. Барабанова, В. И. Кияев. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 162 с. — (Высшее образование). — ISBN 978-5-534-17504-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/533206

2. Замятина, О. М. Вычислительные системы, сети и телекоммуникации. Моделирование сетей: учебное пособие для вузов / О. М. Замятина. — Москва: Издательство Юрайт, 2022. — 167 с. — (Высшее образование). — ISBN 978-5-534-16305-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530772

5. Материально-техническое обеспечение

5.1. Требования к оборудованию и помещению для занятий

Занятия по дисциплине Сети и системы передачи информации должны проводиться в специализированных аудиториях в корпусе Московского Политеха на ул. Прянишникова д.2а, ауд. ПР2402 и ПР2403, оснащенных современной оргтехникой и персональными компьютерами с программным обеспечением в соответствии с тематикой изучаемого материала. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов. Рабочее место преподавателя должно быть оснащены современным компьютером с подключенным к нему проектором на настенный экран, или иным аналогичным по функциональному назначению оборудованием.

5.2. Требования к программному обеспечению

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

- ОС
- Веб-браузер
- Putty
- TerraTerm
- Cisco Packet Tracer

6. Методические рекомендации

6.1. Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведённое для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учётом учебного времени, отведённого для занятия.

2. При проверке работ и отчётов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

3. Для сдачи работ, которые студент не выполнил в течение семестра, преподаватель организует дополнительные занятия в конце семестра.

6.2. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекционные занятия, лабораторные работы.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты и записи, готовятся к проведению и обрабатывают результаты лабораторных работ, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

• защита лабораторных работ;

• контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

• уровень освоения студентом учебного материала;

• умения студента использовать теоретические знания при выполнении практических задач;

• сформированность компетенций;

• оформление материала в соответствии с требованиями.

7. Фонд оценочных средств

7.1. Описание показателей и критериев оценивания

№ ОС	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Контрольный рубеж (устный опрос/ собеседование)	Средство контроля, организованное как очная беседа педагогического работника с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме, в т.ч. по лабораторным работам.	Вопросы по темам/разделам дисциплины. Вопросы по лабораторным работам
2	Контрольный рубеж (письменный опрос)	Средство контроля, организованное как очный письменный ответ обучающегося на темы, связанные с изучаемой дисциплиной, и рассчитанный на выяснение объема знаний	Вопросы по темам/разделам дисциплины. Вопросы по лабораторным работам

		обучающегося по определенному разделу, теме, проблеме, в т.ч. по лабораторным работам.	
4	Тест(Т)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
5	Экзаменационные билеты (ЭБ)	Средство проверки знаний, умений, навыков. Может включать комплекс теоретических вопросов, задач, практических заданий.	Экзаменационные билеты. Шкала оценивания и процедура применения.

7.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем				
ОПК-5.1. Знать: основы системного администрирования. ОПК-5.2. Уметь: выполнять подключение, установку и проверку аппаратных, программно-аппаратных и программных средств. ОПК-5.3. Владеть: методами установки системного и прикладного программного обеспечения.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.
ОПК-7. Способен участвовать в настройке и наладке программно-аппаратных комплексов				
ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть:	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Допускаются значительные ошибки, проявляется	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Но допускаются незначительные ошибки, неточности,	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.

способами проверки работоспособности программно-аппаратных комплексов.		недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	затруднения при аналитических операциях.	
ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения				
ОПК-8.1. Знать: операционные системы и оболочки.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины. Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины.

7.3. Шкала оценивания результатов промежуточной аттестации и её описание.

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Приведенные ниже правила выставления оценок и опозданий могут быть изменены, если преподаватель сочтет это необходимым. Важно, чтобы студенты регулярно просматривали план курса, выложенный в СДО, на предмет его обновления или изменения.

В соответствии с планом дисциплины студентам выдаются задания на лабораторные работы. Лабораторные работы могут состоять из практических заданий, которые требуют выполнения работы в аудитории университета и заданий для самостоятельной работы. Помимо требований и описания задания в работе указан крайний срок сдачи. Для сдачи лабораторной работы студенту необходимо выполнить практическую часть в соответствии с заданием и защитить работу. Во время защиты лабораторной работы преподаватель проверяет

практическую часть работы и опрашивает студента по теоретическим разделам темы лабораторной работы. Если студент отказывается отвечать на вопросы, или дает полностью неверные ответы, или ответы не по теме, то работа может считаться сданной, но при этом она оценивается не выше 1 балла.

Работа должна быть выполнена студентом самостоятельно: на снимках экрана студента должен быть виден рабочий стол, меню пуск с датой и временем и ФИО студента. Если эти правила не соблюдаются, то работа не считается сданной и не оценивается.

Рубежные контроли (устный/письменный опрос) сдаются в аудитории индивидуально по варианту задания, выданному преподавателем в назначенные дни. При отсутствии студента в день написания контрольной работы ему разрешается сдать работу на следующем занятии, при этом студенту начисляется штраф в размере 1 балла, за каждую неделю просрочки.

Каждый студент имеет право на 3 недели опоздания (без начисления штрафных баллов), которые могут быть потрачены на любые задания в течение семестра. Опоздания предназначены для решения особых ситуаций, таких как болезнь или чрезвычайные семейные обстоятельства.

Студенты должны заранее сообщать о том, что у них могут возникнуть трудности со своевременной сдачей задания или проекта. При наличии реальных причин задержки студентам следует как можно скорее связаться с преподавателем и обсудить возможные условия.

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине – выполнение и защита Лабораторных работ согласно полученному заданию, сдача рубежных контролей (устных/письменных опросов/собеседований) по темам учебного курса, выполнение тестов по всем разделам курса, включая итоговый тест в системе ЛМС Московского Политеха с достижением пороговых значений оценок по всем видам учебной работы. При этом используется балльно-рейтинговая система, включающая следующие критерии оценки.

Критерий	**Значение критерия**
Выполнение и защита лабораторных работ в срок. (L)	От 1 до 5 баллов за каждую работу в зависимости от уровня практического выполнения работы и знания теоретического материала. Максимальное значение критерия – не более 25 баллов.
Сдача рубежных контролей по темам курса в срок (устный/письменный опрос/ собеседование),(I)	От 1 до 5 баллов за каждое собеседование в зависимости от уровня и знания теоретического и практического материала. Максимальное значение критерия – не более 25 баллов.
Выполнение тестов по темам курса в системе ЛМС(T1)	По 1 баллу за каждый тест, выполненный более чем на 70% правильных ответов. Максимальное значение критерия – не более 10 баллов. Допускается 3 попытки на каждый тест в течение семестра.
Выполнение итогового теста по всем темам курса в системе ЛМС (T2)	По 1 баллу за каждые 10% правильных ответов в тесте. Минимальное значение критерия – 7 баллов (70% правильных ответов), максимальное значение критерия – 10 баллов (100% правильных ответов).
Посещение занятий (V)	По 1 баллу за присутствие студента на каждом занятии (2 ак. часа) Максимальное значение критерия – 30 баллов.
Коэффициент сданных работ (K)	Коэффициент равен 1, если все работы (лабораторные работы, рубежные контроли, тесты) сданы и 0 если хотя бы одна работа не сдана.
Расчет итогового балла (F)	F=(L+I+T1+T2+V)*K
Выполнение экзаменационного задания	При выборе студентом выполнения экзаменационного задания баллы набранные в течении семестра обнуляются. Максимальное значение критерия – 100 баллов.

Оценка по балльно-рейтинговой системе	**Оценка по итоговой аттестации**
0 … 60	Неудовлетворительно
61 … 75	Удовлетворительно
76 … 90	Хорошо
91 … 100	Отлично

Шкала оценивания	**Описание**
Отлично	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 5. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным

	в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 4. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 3. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не достигнуто пороговое значение хотя бы для одного уровня формируемых на момент проведения аттестации компетенций. Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.4.Описания показателей оценивания и критериев оценивания компетенций

В процессе освоения данной дисциплины студент формирует и демонстрирует следующие общепрофессиональные компетенции:

Компетенции		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средства****	**Степени уровней освоения компетенций**
Индекс	**Индекс**				
ОПК-5	Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем	ОПК-5.1. Знать: основы системного администрирования. ОПК-5.2. Уметь: выполнять подключение, установку и проверку аппаратных, программно-аппаратных и программных средств. ОПК-5.3. Владеть: методами установки системного и прикладного программного обеспечения.	Лабораторные работы, самостоятельная работа	УО П Экзамен	БАЗОВЫЙ УРОВЕНЬ: способность выполнять полученное задание, применяя полученные знание и умения на практике, владеть соответствующим и индикаторами компетенции при выполнении задания. ПРОДВИНУТЫЙ УРОВЕНЬ: способность выполнять полученное задание и решать самостоятельно сформированные задачи, применяя полученные знание и умения на практике. Уверенно владеть соответствующим и индикаторами компетенции при выполнении задания, комбинировать их
ОПК-7	Способен участвовать в настройке и наладке программно-аппаратных комплексов	ОПК-7.1. Знать: методы настройки, наладки программно-аппаратных комплексов. ОПК-7.2. Уметь: производить настройку, наладку и тестирование программно-аппаратных комплексов. ОПК-7.3. Владеть:			

		способами проверки работоспособности программно-аппаратных комплексов.			между собой и с индикаторами других компетенций для достижения проектных результатов.
ОПК-8	Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-8.1. Знать: операционные системы и оболочки.			

**- Сокращения форм оценочных средств см. в приложении 2 к РП.

7.5. Экзаменационное задание.

Форма экзаменационного задания выбирается преподавателем и утверждается на заседании кафедры. Экзамен может проходить в следующих формах и с использованием следующих оценочных средств.

Форма	**Представление оценочного средства в ФОС**
Устная.	Банк контрольных вопросов, соответствующих отдельным темам дисциплины (см. п. 4 настоящего документа). Вопросы формируют экзаменационный билет (см. ниже), состоящий из теоретических вопросов и практических заданий (типовые практические задания представлены ниже). Билеты, включая вопросы и практические задания, формируются преподавателем и утверждаются на заседании кафедры. В них могут быть включены дополнительные контрольные вопросы и задания, не требующие у студентов наличия не формируемых данной дисциплиной компетенций или более высоких этапов сформированности формируемых. Для ответа на каждый вопрос и для решения любого практического задания студент должен находится на требуемом для данной дисциплине уровне сформированности всех соответствующих ей компетенций: каждый вопрос и задание проверяет уровень сформированности всех соответствующих данной дисциплине компетенций.
Письменная.	Оценочное средство полностью соответствует оценочным средствам устной формы задания.

7.6. Список экзаменационных вопросов.

1. Инструменты хакера: Инструменты проведения атак. Категории атак для взлома сети.

2. Распространенные типы (категории) сетевых атак. Техники разведывательных атак. Причины атак для получения доступа. Типы атак для получения доступа. Инструменты социальной инженерии. Основные типы атак «отказ в обслуживании». Наиболее популярные типы DoS-атак. DDoS-атаки.

3. Устранение типичных сетевых атак. Фазы нейтрализации червя. Способы нейтрализации разведывательных атак. Способы нейтрализации атак для получения доступа. Способы нейтрализации DoS-атак.

4. Структура защиты сетевой платформы Cisco. Функции защиты плоскости управления. Функции защиты плоскости менеджмента. Функции защиты плоскости данных.

5. Граничный маршрутизатор. Подходы к защите граничных маршрутизаторов. Три области защиты маршрутизатора. Задачи по защите административного доступа. Меры предосторожности при безопасном локальном и удаленном доступе.

6. Рекомендации по надежным паролям. Алгоритмы хэширования пароля Secret. Защита доступа к линии.

7. Конфигурирование усовершенствованных функций.

Усовершенствование процесса входа в систему. Функции расширенного входа в систему Cisco IOS.

Включение расширенных функций входа в систему. Команда login block-for.

Команды, помогающие обнаружить неудачные попытки входа.

8. Конфигурирование SSH. Требования к маршрутизатору для обеспечения поддержки SSH. Шаги для настройки SSH

9. Назначение административных ролей. Два уровня доступа к командам. 16 уровней привилегий. Ограничения уровней привилегий.

10. Конфигурирование CLI на основе ролей. Преимущества доступа к CLI на основе ролей. Представления команд на основе ролей. Особенности суперпредставления.

11. Защита файлов конфигурации и образа Cisco IOS. Сведения об устойчивой конфигурации Cisco IOS. Команда защиты образа IOS и включения функции отказоустойчивости образа Cisco IOS.

12. Защита управления и отчетности. Определение типа доступа управления. Внутриполосное управление. Внеполосное управление (OOB). Особенности внеполосного (OOB) управления. Особенности внутриполосного управления

13. Использование системного журнала (Syslog) для защиты сети. Основные функции сервиса ведения системного журнала (syslog). Использование системного журнала (Syslog). Уровни опасности Syslog-сообщения. Типы систем Syslog.

14. Использование протокола SNMP для защиты сети. Основные сведения о протоколе SNMP. Элементы системы SNMP. Версии протокола SNMP. Модели и уровни безопасности SNMP. Уязвимости SNMP. Функции безопасности SNMPv3.

15. Использование NTP. Назначение протокола сетевого времени. Сервер NTP.

16. Выполнение аудита безопасности. Рекомендации по настройке протоколов и сервисов

17. Последствия спуфинга информации о маршрутизации

18. Эксплуатация сетевых устройств. Пакеты плоскости данных. Пакеты плоскости управления. Пакеты плоскости менеджмента.

19. Компоненты AAA. Режимы (методы) аутентификации. Авторизация. Учет. Типы учетной информации.

20. Характеристики локальной аутентификации AAA. Шаги по настройке локальной аутентификации AAA.

21. Характеристики серверного решения AAA. Шаги по настройке серверной аутентификации AAA.

22. Сравнение TACACS+ и RADIUS. Основные характеристики TACACS+. Основные характеристики RADIUS. Этапы процесса аутентификации TACACS+. Этапы процесса аутентификации RADIUS.

23. Шаги процедуры настройки серверной аутентификации AAA. Серверная авторизация и учет AAA.

24. Синтаксис команд настройки стандартного нумерованного списка ACL. Синтаксис команд настройки нумерованного расширенного списка ACL.

25. Синтаксис команд настройки именованных стандартных или расширенных списков ACL. Синтаксис команд для применения списка ACL к интерфейсу или к линиям VTY.

26. Указания по настройке и применению списков ACL. Редактирование существующих списков ACL. Порядковые номера и стандартные списки ACL.

27. Синтаксис команды настройки ACL-списка IPv6. Синтаксис команды для применения ACL-список IPv6 к интерфейсу. Указания по настройке и применению ACL-списков IPv6.

28. Определение межсетевых экранов. Преимущества и ограничения межсетевых экранов.

29. Типы межсетевых экранов. Преимущества и ограничения межсетевых экранов с фильтрацией пакетов.

30. Межсетевые экраны с сохранением состояния. Преимущества и ограничения межсетевых экранов с сохранением состояния.

31. Принцип работы классического межсетевого экрана.

32. Системы обнаружения вторжений (Intrusion Detection Systems, IDS). Системы предотвращения вторжений (Intrusion Prevention Systems, IPS). Преимущества и недостатки систем IDS. Преимущества и недостатки IPS.

33. Хостовая реализация IPS. Преимущества и недостатки хостовой реализации системы IPS.

34. Сетевая реализация IPS. Преимущества и недостатки сетевой реализации системы IPS.

35. Характеристики сигнатур для IPS-систем: атрибуты сигнатур, типы сигнатур.
36. Сигналы (триггеры) тревоги сигнатур IPS. Сравнение триггеров сигнатур.
37. Обнаружение на основе шаблона.
38. Обнаружение на основе аномалий.
39. Обнаружение на основе политик и обнаружение с помощью Honey Pot.
40. Механизмы инициирования сигналов тревоги.
41. Действия сигнатур IPS.
42. Категории атак на коммутаторы.
43. Пример работы таблицы CAM. Атаки на таблицу CAM.
44. Нейтрализация атак на таблицы CAM. Защита портов. Включение опций защиты портов.
45. Режимы нарушения защиты портов. Сравнение режимов нарушения защиты.
46. Атаки перехода (Hopping) VLAN.
47. Атака с двойным тегированием (Double-Tagging) VLAN.
48. Нейтрализация атак перехода VLAN.
49. Спуфинг DHCP.
50. Истощение DHCP.
51. Спуфинг ARP и ARP Poisoning.
52. Спуфинг MAC-адресов.
53. Протокол связующего дерева. Атаки путем манипуляций STP.
54. Основные задачи защиты обмена данными: аутентификация, целостность и конфиденциальность.
55. Криптографическая хеш-функция.
56. Свойства криптографической хеш-функции
57. Алгоритм хеширования Message Digest 5
58. Аутентификация с помощью алгоритма HMAC. Код аутентификации сообщения на основе хеш-функции (Keyed-Hash Message Authentication Code, HMAC).
59. Методики тестирования безопасности сети.
60. Перечень задач по тестированию и оценке безопасности сети.
61. Типы сетевых тестов.
62. Применение результатов тестирования сети.
63. Инструменты тестирования безопасности сети.
64. Инструменты тестирования сети.

7.7.Примерный список вопросов для контрольных рубежей и защиты лабораторных работ

Тема 1

1. Инструменты хакера: Инструменты проведения атак. Категории атак для взлома сети.

2. Распространенные типы (категории) сетевых атак. Техники разведывательных атак. Причины атак для получения доступа. Типы атак для получения доступа. Инструменты социальной инженерии. Основные типы атак «отказ в обслуживании». Наиболее популярные типы DoS-атак. DDoS-атаки.

3. Устранение типичных сетевых атак. Фазы нейтрализации червя. Способы нейтрализации разведывательных атак. Способы нейтрализации атак для получения доступа. Способы нейтрализации DoS-атак.

4. Структура защиты сетевой платформы Cisco. Функции защиты плоскости управления. Функции защиты плоскости менеджмента. Функции защиты плоскости данных.

Тема 2

1. Граничный маршрутизатор. Подходы к защите граничных маршрутизаторов. Три области защиты маршрутизатора. Задачи по защите административного доступа. Меры предосторожности при безопасном локальном и удаленном доступе.

2. Рекомендации по надежным паролям. Алгоритмы хэширования пароля Secret. Защита доступа к линии.

3. Конфигурирование усовершенствованных функций.

Усовершенствование процесса входа в систему. Функции расширенного входа в систему Cisco IOS.

Включение расширенных функций входа в систему. Команда login block-for.

Команды, помогающие обнаружить неудачные попытки входа.

4. Конфигурирование SSH. Требования к маршрутизатору для обеспечения поддержки SSH. Шаги для настройки SSH

5. Назначение административных ролей. Два уровня доступа к командам. 16 уровней привилегий. Ограничения уровней привилегий.

6. Конфигурирование CLI на основе ролей. Преимущества доступа к CLI на основе ролей. Представления команд на основе ролей. Особенности суперпредставления.

7. Защита файлов конфигурации и образа Cisco IOS. Сведения об устойчивой конфигурации Cisco IOS. Команда защиты образа IOS и включения функции отказоустойчивости образа Cisco IOS.

8. Защита управления и отчетности. Определение типа доступа управления. Внутриполосное управление. Внеполосное управление (OOB). Особенности внеполосного (OOB) управления. Особенности внутриполосного управления

9. Использование системного журнала (Syslog) для защиты сети. Основные функции сервиса ведения системного журнала (syslog). Использование системного журнала (Syslog). Уровни опасности Syslog-сообщения. Типы систем Syslog.

10. Использование протокола SNMP для защиты сети. Основные сведения о протоколе SNMP. Элементы системы SNMP. Версии протокола SNMP. Модели и уровни безопасности SNMP. Уязвимости SNMP. Функции безопасности SNMPv3.

11. Использование NTP. Назначение протокола сетевого времени. Сервер NTP.

12. Выполнение аудита безопасности. Рекомендации по настройке протоколов и сервисов

13. Последствия спуфинга информации о маршрутизации

14. Эксплуатация сетевых устройств. Пакеты плоскости данных. Пакеты плоскости управления. Пакеты плоскости менеджмента.

Тема 3

1. Компоненты AAA. Режимы (методы) аутентификации. Авторизация. Учет. Типы учетной информации.

2. Характеристики локальной аутентификации AAA. Шаги по настройке локальной аутентификации AAA.

3. Характеристики серверного решения AAA. Шаги по настройке серверной аутентификации AAA.

4. Сравнение TACACS+ и RADIUS. Основные характеристики TACACS+. Основные характеристики RADIUS. Этапы процесса аутентификации TACACS+. Этапы процесса аутентификации RADIUS.

5. Шаги процедуры настройки серверной аутентификации AAA. Серверная авторизация и учет AAA.

Тема 4

1. Синтаксис команд настройки стандартного нумерованного списка ACL. Синтаксис команд настройки нумерованного расширенного списка ACL.

2. Синтаксис команд настройки именованных стандартных или расширенных списков ACL. Синтаксис команд для применения списка ACL к интерфейсу или к линиям VTY.

3. Указания по настройке и применению списков ACL. Редактирование существующих списков ACL. Порядковые номера и стандартные списки ACL.

4. Синтаксис команды настройки ACL-списка IPv6. Синтаксис команды для применения ACL-список IPv6 к интерфейсу. Указания по настройке и применению ACL-списков IPv6.

5. Определение межсетевых экранов. Преимущества и ограничения межсетевых экранов.

6. Типы межсетевых экранов. Преимущества и ограничения межсетевых экранов с фильтрацией пакетов.

7. Межсетевые экраны с сохранением состояния. Преимущества и ограничения межсетевых экранов с сохранением состояния.

8. Принцип работы классического межсетевого экрана.

Тема 5

1. Системы обнаружения вторжений (Intrusion Detection Systems, IDS). Системы предотвращения вторжений (Intrusion Prevention Systems, IPS). Преимущества и недостатки систем IDS. Преимущества и недостатки IPS.

2. Хостовая реализация IPS. Преимущества и недостатки хостовой реализации системы IPS.

3. Сетевая реализация IPS. Преимущества и недостатки сетевой реализации системы IPS.

4. Характеристики сигнатур для IPS-систем: атрибуты сигнатур, типы сигнатур.

5. Сигналы (триггеры) тревоги сигнатур IPS. Сравнение триггеров сигнатур.

6. Обнаружение на основе шаблона.

7. Обнаружение на основе аномалий.

8. Обнаружение на основе политик и обнаружение с помощью Honey Pot.

9. Механизмы инициирования сигналов тревоги.

10. Действия сигнатур IPS.

Тема 6

1. Категории атак на коммутаторы.

2. Пример работы таблицы CAM. Атаки на таблицу CAM.

3. Нейтрализация атак на таблицы CAM. Защита портов. Включение опций защиты портов.

4. Режимы нарушения защиты портов. Сравнение режимов нарушения защиты.

5. Атаки перехода (Hopping) VLAN.

6. Атака с двойным тегированием (Double-Tagging) VLAN.

7. Нейтрализация атак перехода VLAN.

8. Спуфинг DHCP.

9. Истощение DHCP.

10. Спуфинг ARP и ARP Poisoning.

11. Спуфинг MAC-адресов.

12. Протокол связующего дерева. Атаки путем манипуляций STP.

Тема 7

1. Основные задачи защиты обмена данными: аутентификация, целостность и конфиденциальность.

2. Криптографическая хеш-функция.

3. Свойства криптографической хеш-функции

4. Алгоритм хеширования Message Digest 5

5. Аутентификация с помощью алгоритма HMAC. Код аутентификации сообщения на основе хеш-функции (Keyed-Hash Message Authentication Code, HMAC).

Тема 8

1. Методики тестирования безопасности сети.

2. Перечень задач по тестированию и оценке безопасности сети.

3. Типы сетевых тестов.

4. Применение результатов тестирования сети.

5. Инструменты тестирования безопасности сети.

6. Инструменты тестирования сети.

7.8.Пример из теста в системе ЛМС.

Правила контроля доступа (ACE). Выберите правильные утверждения:

порядок правил имеет большое значение, так как обработка ACL-списков выполняется сверху вниз

только один ACL разрешен для каждого интерфейса, для каждого протокола, в каждом направлении.

новые правила для существующего списка ACL добавляются по умолчанию вниз списка ACL

генерируемые маршрутизатором пакеты не фильтруются исходящими ACL-списками

стандартные ACL-списки следует размещать как можно ближе к месту назначения.

расширенные ACL-списки следует размещать как можно ближе к источнику

7.9.Пример оформления экзаменационного билета

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Московский политехнический университет»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
по дисциплине
«Сети и системы передачи информации»
направление подготовки 09.03.01
«Информатика и вычислительная техника»

ВОПРОСЫ:

1. Основные задачи защиты обмена данными: аутентификация, целостность и конфиденциальность.
2. Спуфинг DHCP. Истощение DHCP. Спуфинг ARP и ARP Poisoning. Спуфинг MAC-адресов.
3. Методики тестирования безопасности сети.

Утверждено: _____ / _____ / «__» _____ 20__г.