Приложение к ОПОП «Безопасность и этика искусственного интеллекта»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)

РАБОЧАЯ ПРОГРАММА

дисциплины

«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ»

для подготовки магистров

по направлению

09.04.01 «Информатика и вычислительная техника»

по программе

«Безопасность и этика искусственного интеллекта»

Санкт-Петербург

2021

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

к.т.н., доцент Фаткиева Р.Р.

Рабочая программа рассмотрена и одобрена на заседании кафедры ВТ 02.09.2021, протокол № 6

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 16.09.2021, протокол № 6

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	ИБ
Общая трудоемкость (ЗЕТ)	4
Курс	2
Семестр	3
Виды занятий	
Лекции (академ. часов)	17
Практические занятия (академ. часов)	34
Все контактные часы (академ. часов)	51
Самостоятельная работа, включая часы на контроль (академ. часов)	93
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	2

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ»

Дисциплина посвящена основным принципам построения защищенных телекоммуникаций. В содержание дисциплины входят основные направления обеспечения защиты компьютерных сетей: обнаружение компьютерных атак, межсетевое экранирование, организация виртуальных частных сетей, технологии предотвращения вторжений, основанные на методах интеллектуального аудита информационной безопасности. В ходе изучения студенты получают знания о базовых принципах обеспечения защиты информации при ее передаче и приобретают навыки, необходимые для практического построения и администрирования защищенных компьютерных сетей с применением современных средств защиты информации. Полученные знания позволяют правильно ориентироваться в многообразии выпускаемых и предлагаемых программно-аппаратных средств сетевой защиты.

SUBJECT SUMMARY

«BASICS FOR BUILDING SECURE COMPUTER NETWORKS»

The discipline is devoted to the basic principles of building secure telecommunications. The content of the discipline includes the main areas of ensuring the protection of computer networks: detection of computer attacks, firewall shielding, organization of virtual private networks, intrusion prevention technologies based on the methods of intelligent audit of information security. During the study, students gain knowledge of the basic principles of ensuring the protection of information during its transmission and acquire the skills necessary for the practical construction and administration of secure computer networks using modern means of information protection. The acquired knowledge allows you to correctly navigate the variety of available and offered software and hardware network protection.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Дисциплина формирует знания и практические навыки, необходимые для построения защищенных компьютерных сетей, в составе которых имеются криптографические, программно-аппаратные методы обеспечения информационной безопасности в компьютерных системах.

2. Предметом изучения являются сетевые системы передачи данных по защищенным каналам связи для обеспечения конфиденциальности и целостности информации, циркулирующей в сети. Теоретический базис дисциплины основывается на знаниях из теории кодирования, теории криптографических алгоритмов и особенностей их программной реализации, теории машинного обучения.

3. В результате освоения дисциплины у студента должно быть сформировано знание: основных протоколов передачи данных; механизмов реализации атак в сетях и средств обеспечения безопасности компьютерных сетей; протоколов идентификации и аутентификации, применяемых для обеспечения безопасности в сети; средств и методов предотвращения и обнаружения вторжений; основных требований нормативно-правовой базы к защите компьютерных сетей.

4. В результате изучения дисциплины студенты должны владеть: умением анализировать и оценивать угрозы информационной безопасности объекта и противодействовать нарушениям сетевой безопасности.

5. Результатом освоения дисциплины является приобретение практических навыков настройки программных и аппаратных средств при построении компьютерных сетей, использующих криптографическую и интеллектуальную защиту информации.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Аналитическая обработка данных в задачах информационной безопасности»

2. «Криптография и криптографические протоколы»

3. «Машинное обучение»

и обеспечивает подготовку выпускной квалификационной работы.

3.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ПК-27	Способен руководить проектами по созданию комплексных систем искусственного интеллекта
ПК-27.1	*Руководит разработкой архитектуры комплексных систем искусственного интеллекта*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	СР, ач
1	Введение. Основные принципы построения защищенных систем	1	2	4
2	Виды нарушений сетевой безопасности	2		12
3	Сетевые протоколы передачи информации	2	8	10
4	Межсетевое экранирование	2	8	12
5	Виртуальные частные сети	2	4	12
6	Протоколы идентификации, аутентификации и авторизации	1	2	4
7	Средства и методы интеллектуального обнаружения и предотвращения вторжений	4	6	26
8	Беспроводные технологии	2	4	12
9	Заключение	1		1
	Итого, ач	17	34	93
	Из них ач на контроль	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4		

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение. Основные принципы построения защищенных систем	Теоретические основы построения защищенных сетей. Основные элементы многоуровневой системы обеспечения защиты при передаче информации по каналам связи
2	Виды нарушений сетевой безопасности	Обзор и анализ существующих стандартов в области обеспечения сетевого взаимодействия. Модель угроз и модель нарушителя информационной безопасности компьютерной сети. Сетевые атаки. Классификация сетевых атак. Механизмы реализации атак в сетях. Формирование требования к средствам защиты при построении защищённых компьютерных сетей. Основные этапы разработки проектных решений по системам обеспечения информационной безопасности на базе компьютерных сетей.

№ п/п	Наименование темы дисциплины	Содержание
3	Сетевые протоколы передачи информации	Способы передачи данных по сети. Топологии сети. Эталонная модель взаимодействия открытых систем (ISO OSI). Уровни и протоколы. Стек протоколов TCP/IP. Виды сетевого оборудования для построения сегментированной сети (сетевые адаптеры, коммутаторы, маршрутизаторы). Виды маршрутизации трафика. Протоколы маршрутизации.
4	Межсетевое экранирование	Классификация межсетевых экранов. Основные компоненты межсетевых экранов и особенности их функционирования. Классификации: управляемые коммутаторы, пакетные фильтры, шлюзы сеансового уровня, посредники прикладного уровня, инспекторы состояния. Технология NAT. Правила фильтрации сетевого контента и способы ограничения доступа к сетевой инфраструктуре.
5	Виртуальные частные сети	Определение виртуальной частной сети (VPN). Преимущества VPN. Типы VPN-сетей. Виртуальные частные сети канального уровня. Протоколы PPTP, L2TP принцип работы, настройка. Технологии туннелирования. Протоколы IPSec. Сервисы безопасности IPsec.
6	Протоколы идентификации, аутентификации и авторизации	Средства и методы хранения и передачи аутентификационной информации. Обеспечение защиты с использованием протоколов PAP, CHAP.
7	Средства и методы интеллектуального обнаружения и предотвращения вторжений	Архитектура систем обнаружения вторжения. Пассивные и активные системы обнаружения вторжения, системы мониторинга сети (IDS/IPS). Многоагентные системы обнаружения вторжений. Методы машинного обучения для оценки сетевого трафика (линейная регрессия и кластеризация, анализ временных рядов, баесовский классификатор) Использование нейронных сетей для обнаружения сетевых атак. Методы прогнозирования сетевого трафика. Модели программно-конфигурируемых сетей
8	Беспроводные технологии	Теоретические основы построения и архитектура беспроводных сетей. Безопасность передачи данных в беспроводных технологиях. . Реализация безопасности беспроводных сетей. Алгоритмы WEP, WPA и WPA 2, RC4.
9	Заключение	Модернизации объектов информатизации на базе компьютерных сетей в защищенном исполнении.

4.2 Перечень лабораторных работ

Лабораторные работы не предусмотрены.

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Основные принципы построения защищенных сетей. Проектирование защищенной компьютерной сети.	4
2. Основные принципы построения защищенных сетей. Настройка операционной системы Cisco IOS. Пользовательский и административный режимы. Режимы конфигурирования	8
3. Сетевые протоколы передачи информации. Развертывание сети с использованием VLAN. Настройка сетевого оборудования. Защита инфраструктуры коммутации. Защита ЛВС от петель на канальном уровне	8
4. Протоколы идентификации, аутентификации и авторизации. Построение маршрутизируемой ЛВС. Защита сетевой инфраструктуры. Настройка аутентификации маршрутизаторов	4
5. Межсетевое экранирование. Настройка ACL-списков на маршрутизаторе Cisco. Настройка NAT на межсетевом экране Cisco	6
6. Беспроводные технологии. Построение защищенного сегмента беспроводной сети с использованием механизмов WPA2.	4
Итого	34

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Индивидуальное домашнее задание не предусмотрено.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины.

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	20
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	0
Самостоятельное изучение разделов дисциплины	14
Выполнение домашних заданий, домашних контрольных работ	0
Подготовка к лабораторным работам, к практическим и семинарским занятиям	4
Подготовка к контрольным работам, коллоквиумам	12
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	4
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	4
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	93

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Таненбаум, Эндрю. Компьютерные сети [Текст] : учебное пособие / Э. Таненбаум; [Пер. с англ. В. Шрага], 2003. -991 с.	60
2	Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы [Текст] : учеб. пособие для вузов по направлению ”Информатика и вычислит. техника” и по специальности ” Вычислит. машины, комплексы, системы и сети”, ”Автоматизир. машины, комплексы, системы и сети”, ” Програм. обеспечение вычислит. техники и автоматизир. систем” / В.Г. Олифер, Н.А. Олифер, 2006. -957 с.	133
3	Борисенко, Константин Алексеевич. Сети и телекоммуникации [Текст] / К. А. Борисенко, 2021. -43 с.	50
4	Дибров, Максим Владимирович. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 [Электронный ресурс] : Учебник и практикум для вузов / Дибров М. В., 2021. -351 с	неогр.
5	Дибров, Максим Владимирович. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 [Электронный ресурс] : Учебник и практикум для вузов / Дибров М. В., 2021. -333 с	неогр.
6	Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов [Электронный ресурс] / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова, 2018. -220 с.	неогр.
Дополнительная литература		
1	Фирсов, Михаил Александрович. Коммутация и маршрутизация в IP-сетях, виртуальные локальные сети [Текст] : учеб. пособие / М. А. Фирсов, В. В. Яновский, 2018. -85 с.	38
2	Дернова, Евгения Сергеевна. Криптографические протоколы [Текст] : учеб. пособие / Е.С. Дернова, Д.Н. Молдовян, Н.А. Молдовян, 2010. -99 с	неогр.

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Электронный портал центра обучения «Cisco Learning Locator» https://learninglocator.cloudapps.cisco.com/#/home
2	Обучающий курс по сетевым технологиям https://easy-network.ru/

№ п/п	Электронный адрес
3	Обучающий курс по компьютерным сетям https://openedu.ru/course/bmstu/MGTU_8/
4	Практический курс работы в симуляторе Cisco Packet Tracer http://blog.netskills.ru

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=7531

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Основы построения защищенных компьютерных сетей» формой промежуточной аттестации является экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	Оценка «неудовлетворительно» выставляется студенту, продемонстрировавшему существенные пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий.
Удовлетворительно	Оценка «удовлетворительно» выставляется студенту, продемонстрировавшему знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой, обладающему необходимыми знаниями, но допустившему неточности в ответах на аттестационном испытании и при выполнении учебных заданий.
Хорошо	Оценка «хорошо» выставляется студенту, продемонстрировавшему полное знание учебного материала, успешно выполнившему предусмотренные программой задачи, освоившему основную рекомендованную литературу, показавшему систематический характер знаний по дисциплине и способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности.
Отлично	Оценка «отлично» выставляется студенту, продемонстрировавшему всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, освоившему основную литературу и ознакомившемуся с дополнительной литературой,рекомендованной рабочей программой дисциплины, усвоившему взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании, изложении и использовании учебного материала

Особенности допуска

Основным требованием для получения допуска к экзамену является успешное выполнение и защита на коллоквиуме 6 практических работ.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Примерные вопросы к экзамену

№ п/п	Описание
1	Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных. Модель угроз информационной безопасности компьютерной сети. Модель нарушителя информационной безопасности компьютерной сети.
2	Базовая модель взаимодействия сетевых приложений. Обеспечение безопасности модели сетевого взаимодействия OSI. Сетевые атаки. Классификация сетевых атак.
3	Механизмы реализации атак в сетях. Механизмы реализации атак в сетях, реализующих протоколы транспортного и сетевого уровня.
4	Обеспечение безопасности протокола TCP/IP. Механизмы реализации атак в сетях, реализующих протоколы прикладного уровня.
5	Обеспечение защиты уровня межсетевого взаимодействия стека протоколов TCP/IP. Обеспечение защиты транспортного уровня стека протоколов TCP/IP.
6	Теоретические и практические основы обеспечения сегментирования сети и использования технологии VLAN (сегментирование и зонирование сети, управления доменами и учетными записями домена).
7	Виды маршрутизации трафика. Протоколы маршрутизации. Теоретические и практические основы построения сетевого взаимодействия с резервированием каналов при передаче данных.
8	Протоколы управления сетью. Атаки на протокол ICMP. Методы обеспечения безопасности.
9	Защита сетевого трафика в локальных сетях. Использование интеллектуальных концентраторов.
10	Понятие межсетевых экранов. Компоненты межсетевого экрана. Технология NAT: основные функции, типы и принципы.
11	Классификации межсетевых экранов: управляемые коммутаторы, пакетные фильтры, шлюзы сеансового уровня, посредники прикладного уровня, инспекторы состояния. Правила фильтрации сетевого контента и способы ограничения доступа к сетевой инфраструктуре.
12	Основные схемы защиты сетевой инфраструктуры на базе межсетевых экранов.
13	Создание защищенных сегментов сетей с использованием межсетевых экранов. Политика сетевой безопасности.
14	Обзор и основные параметры, характеристики и область применения криптографических алгоритмов. Протоколы SSL/TLS. Устройство, принцип работы протокола SSL.
15	Характеристики и область применения криптографических алгоритмов

16	Обзор и основные параметры, характеристики протокола IPsec. Туннельный и транспортный режимы использования.
17	Определение виртуальной частной сети (VPN). Преимущества VPN. Типы VPN-сетей.
18	Виртуальные частные сети канального уровня. Протоколы PPTP, L2TP принцип работы, настройка. Технологии туннелирования.
19	Технология аутентификации. Обеспечение защиты с использованием протоколов PAP, CHAP, IPsec.
20	Основы настройки доступа к маршрутизатору по технологии AAA
21	Активные атаки на беспроводное соединение. Реализация безопасности беспроводных сетей.
22	Теоретические основы построения и архитектура беспроводных сетей. Расположение точек доступа.
23	Теоретические основы построения и архитектура беспроводных сетей. Безопасность передачи данных в беспроводных технологиях. Алгоритм Wired Equivalent Privacy (WEP).
24	Формат кадра, ключи, инкапсуляция и декапсуляция алгоритма WEP.
25	Технология Wi-Fi Protected Access (WPA и WPA 2).
26	Обеспечение защиты стека протоколов Bluetooth.
27	Методы анализа сетевого трафика. Идентификация уязвимостей сетевых приложений по косвенным признакам
28	Методы машинного обучения для оценки сетевого трафика (линейная регрессия и кластеризация, анализ временных рядов, баесовский классификатор)
29	Методы прогнозирования сетевого трафика.
30	Архитектура систем обнаружения вторжения.
31	Использование нейронных сетей для обнаружения сетевых атак

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

Дисциплина **Основы построения защищённых компьютерных сетей** ФКТИ

1. Базовая модель взаимодействия сетевых приложений. Обеспечение безопасности модели сетевого взаимодействия OSI.

2. Основные схемы защиты сетевой инфраструктуры на базе межсетевых экранов

3. Архитектура систем обнаружения вторжения.

УТВЕРЖДАЮ

Заведующий кафедрой

Образцы задач (заданий) для контрольных (проверочных) работ

№ 1-2. Вопросы коллоквиума. Тема: Введение. Основные принципы построения защищенных сетей.

1. Теоретические основы построения защищенных сетей. Планирование сети.

2. Нормативно-правовое обеспечение при построении защищённой сети. Обзор и анализ существующих стандартов в области обеспечения сетевого взаимодействия.

3. Модель угроз и модель нарушителя информационной безопасности компьютерной сети.

4. Сетевые атаки. Классификация сетевых атак.

5. Механизмы реализации атак в сетях.

6. Формирование требования к средствам защиты при построении защищённых компьютерных сетей.

7. Основные этапы разработки проектных решений по системам обеспечения информационной безопасности на базе компьютерных сетей.

8. Программно-аппаратные средства хранения данных.

9. Типы оборудования при передаче данных. Обеспечение безопасности.

10. Основные элементы многоуровневой системы обеспечения защиты

при передаче информации по каналам связи.

№ 3. Вопросы коллоквиума. Тема: Сетевые протоколы передачи информации.

1. Эталонная модель взаимодействия открытых систем (ISO OSI). Уровни и протоколы.

2. Стек протоколов TCP/IP. Обеспечение безопасности стека протокола TCP/IP.

4. Протокол HTTP. Обеспечение защиты клиент-серверного соединения.

3. Теоретические и практические основы обеспечения сегментирования сети и использования технологии VLAN (сегментирование и зонирование сети, управления доменами и учетными записями домена).

4. Виды маршрутизации трафика. Протоколы маршрутизации.

5. Протоколы управления сетью.

6. Технологии резервирования каналов связи. Механизмы обеспечения пропускной способности.

7. Атаки на протокол ICMP. Методы обеспечения безопасности.

8. Определить класс, номер сети и номер узла. IP-адрес 192.168.169.36

9. Вычислить номер сети и номер узла для адреса 192.168.74.66 и маски 255.255.255.192

10. Маска 255.255.240.0 и номер сети 67.38.160.0. Определить соответствующий блок адресов и их количество.

11. Определить полную маску, если ее краткая запись выглядит как /15.

№ 4. Вопросы коллоквиума. Тема: Протоколы идентификации, аутентификации и авторизации.

1. Средства передачи аутентификационной информации.

2. Обеспечение защиты с использованием протоколов PAP, CHAP.

3. Обеспечение защиты с использованием протокола PAP.

4. Обеспечение защиты с использованием протокола CHAP.

5. Обеспечение защиты с использованием протокола IPsec.

6. Обеспечение механизмов авторизации.

7. Механизмы аутентификации при настройке маршрутизации трафика (аутентификация маршрутизаторов).

8. Аутентификация коммутаторов.

9. Основы настройки доступа к маршрутизатору по технологии AAA.

10. Настройка механизмов аутентификации при клиент-серверном соединении.

№ 5. Вопросы коллоквиума. Тема: Межсетевое экранирование.

1. Основные компоненты межсетевых экранов и особенности их функционирования.

2. Технология NAT.

3. Правила фильтрации сетевого контента и способы ограничения доступа к сетевой инфраструктуре.

4. Создание защищенных сегментов сетей с использованием межсетевых экранов. Политика сетевой безопасности.

5. Определение виртуальной частной сети (VPN). Преимущества VPN.

6. Типы VPN-сетей. Технология туннелирования.

7. Виртуальные частные сети канального уровня.

8. Протоколы PPTP, L2TP принцип работы, настройка.

9. Технологии туннелирования. Протоколы IPSec. Сервисы безопасности

IPsec.

10. Опишите результат ввода команды iproute 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе.

11. Опишите результат ввода команды: router(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 eq 80 10.1.1.0 0.0.0.255 eq 443

12. Опишите результат ввода команды: router(config)#access-list 100 deny tcp any host 172.16.1.5 gt 5000

13. Опишите результат ввода команды: access-list 2 deny 194.12.34.0 0.0.0.255 access-list 2 deny 132.7.0.0 0.0.255.255 access-list 2 permit any

14. Применение стандартных списков доступа.

15. Применение расширенных списков доступа.

№ 6. Вопросы коллоквиума. Тема: Беспроводные технологии.

1. Теоретические основы построения и архитектура беспроводных сетей.

2. Безопасность передачи данных в беспроводных технологиях.

3. Виды каналов. Уплотнение с частотным и временным разделением.

4. Беспроводные технологии. Wi-Fi. Метод доступа CSMA/CA и проблема скрытого узла.

5. Построение сети Wi-fi в защищенном исполнении.

6. Обеспечение защиты стека протоколов Bluetooth.

7. Алгоритм WEP.

8. Алгоритмы WPA и WPA 2.

9. Методы анализа сетевого трафика. Идентификация уязвимостей сетевых приложений по косвенным признакам.

10. Методы прогнозирования сетевого трафика.

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
2	Введение. Основные принципы построения защищенных систем	Коллоквиум
3	Введение. Основные принципы построения защищенных систем	Коллоквиум
4	Сетевые протоколы передачи информации	Коллоквиум
5	Протоколы идентификации, аутентификации и авторизации	Коллоквиум
6	Межсетевое экранирование	Коллоквиум
7	Беспроводные технологии	Коллоквиум

6.4 Методика текущего контроля

Текущий контроль включает в себя контроль посещаемости (не менее 80 % занятий).

на практических занятиях

Порядок выполнения практических работ, подготовки отчетов и их защиты.

В процессе обучения по дисциплине «Основы построения защищенных компьютерных сетей» студент обязан выполнить 6 практических работ. Под выполнением практических работ подразумевается подготовка к работе, проведение экспериментальных исследований, подготовка отчета и его защита на коллоквиуме. После каждых практических работ предусматривается проведение коллоквиума на 2, 3, 4, 5, 6, 7 неделях, на которых осуществляется их защита работ. Выполнение практических работ студентами осуществляется в бригадах до 2 человек. Оформление отчета студентами осуществляется индивидуально в соответствии с принятыми в СПбГЭТУ правилами оформления студенческих работ. Отчет оформляется после выполнения экспериментальных исследований и представляется преподавателю на проверку. После проверки отчет либо возвращается (при наличии замечаний) на доработку, либо подписывается к защите.

Практические работы защищаются студентами индивидуально. Каждый

студент получает вопрос по теоретической и практической части после чего ему предоставляется время для подготовки ответа. На защите практической работы студент должен показать: понимание и умение объяснять особенности применяемых методов, возможные области их применения и т.д., прогнозировать реакции исследуемого объекта на различные воздействия, навыки и умения, приобретенные при выполнении практических работы. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов. В случае если студент демонстрирует достаточное знание вопроса, работа считается зачтенной.

Текущий контроль включает в себя выполнение, сдачу в срок отчетов и их защиту по всем практическим работам, по результатам которой студент получает допуск к экзамену.

Критерием оценки работы на коллоквиумах является оценка, выставляемая по 5-ти балльной шкале в соответствии со следующими критериями:

оценка в 5 баллов выставляется при отличном выполнении задания, то есть при наличии полных (с детальными пояснениями и выкладками), оригинальных и правильных решений задач, дополненных при необходимости документами, полученными в результате реализации (проверки) решения, верных ответов и высококачественного оформления работы.

оценка в 4 балла выставляется при правильном выполнении задания, то есть при наличии полных (с пояснениями и выкладками), оригинальных и правильных решений задач, дополненных при необходимости документами, полученными в результате реализации (проверки) решения, верных ответов.

Оценка в 3 балла выставляется при наличии отдельных неточностей в ответах (включая грамматические ошибки) или неточностях в решении задач непринципиального характера (описки и случайные ошибки арифметического характера).

Оценка в 2 и ниже баллов выставляется в случаях, когда в ответах и в решениях задач имеются неточности и ошибки, свидетельствующие о недостаточном понимании вопросов и требующие дополнительного обращения к тематическим материалам.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных, лабораторных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, меловая или маркерная, или электронная доска, компьютер или ноутбук, подключенные к проектору для пока-за презентаций	1) Windows 7 и выше; 2) Microsoft Office 2007 и выше 3) СДО ”Moodle”
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, лабораторный стенд (не менее 14 шт.) на базе компьютера с анализатором сетевого трафика, системой коммуникационного взаимодействия (Cisco) и и аппаратным анализатором сетевых протоколов.	1) ОС Windows 7 и выше; 2)VirtualBox; Wireshark, 3) Cisco Packet Tracer; 4) Microsoft Office 2007 и выше
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows 7 и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА