Методические указания для студентов

Лекционный курс

Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. В конспекте следует применять сокращение слов, что ускоряет запись. Необходимо активно работать с конспектом лекции: после окончания лекции рекомендуется перечитать свои записи, внести поправки и дополнения на полях. Конспекты лекций следует использовать при подготовке к семинарам, при подготовке к опросу, зачету с оценкой, при выполнении самостоятельных заданий.

Практические (семинарские) занятия

№	Наименование практических занятий (семинаров)
1	Бинарное кодирование
2	Тринарное кодирование
3	Тетрарное кодирование
4	Кодирование с использованием кодов замещения
5	Амплитудная цифровая модуляция
6	Частотная модуляция
7	Фазовая модуляция
8	Квадратурная модуляция, QAM-16
9	Повышение производительности локальных сетей на основе методов анализа сетевого трафика
10	Протокол динамической конфигурации хоста DHCP
11	Работа службы разрешения имён NETBIOS WINS (Windows Internet Naming Service)
12	Влияние трафика файлового сеанса связи на работу сети
13	Обзор в корпоративной сети
14	Анализ трафика входа пользователя в систему
15	Работа с DNS
16	Анализ трафика просмотра интрасети

Практические занятия по курсу «Сетевая безопасность» имеют цель познакомить студентов с современным состоянием научной и практической области, связанной с проблемами, методологией, теориями, задачами, технологиями, инструментами и накопленным опытом, используемыми в системах защиты информационных ресурсов. В ходе изучения курса «Сетевая безопасность» особое значение имеют практические занятия, включающие тренинги по использованию различных методов и способов идентификации, аутентификации,

авторизации, шифрования, методов анализа сетевого трафика при выявлении и устранении сетевых атак.

Прохождение всего цикла семинарских занятий является условием допуска студента к зачету с оценкой.

Студент должен вести активную познавательную работу, которая заключается в применении лабораторных стендов, программно-аппаратных комплексов, сетевых топологий, ориентированных на решение научных, проектных и технологических задач; анализа текущего состояния эксплуатируемых корпоративных сетей передачи данных.

Тематика вопросов, рассматриваемых в ходе выполнения практических работ:

- Концептуальные подходы к оптимизации работы компьютерных сетей;
- Методы планирования растущих потребностей в пропускной способности сети;
- Методы и технологии анализа сетевого трафика;
- Обзор нескольких, наиболее востребованных сетевых служб;
- Структура кадров Ethernet;
- Сравнительный анализ протоколов сетевого уровня;
- Функциональные возможности анализатора сетевого трафика Wireshark Network analyzer.
- Методы упрощённого динамического конфигурирования в сетях с протоколом TCP/IP;
- Порядок выделения адресов клиентам DHCP;
- Конфигурация сервера DHCP и его рабочие области;
- Работа с несколькими подсетями и конфигурирование областей;
- Агент-ретранслятор DHCP;
- Диагностика DHCP;
- Влияние трафика DHCP на работу сети: выделение IP-адреса, возобновление IP-адреса;
- Оптимизация трафика DHCP;
- Захват пакетов DHCP из лабораторной сети при помощи ПО Network Analyzer;
- Анализ трафика выделения адреса DHCP сервером;
- Анализ трафика возобновления адреса.
- Четыре способа разрешения имён NETBIOS поверх TCP/IP;
- Серверы и клиенты WINS;
- Репликация баз данных WINS;
- Влияние трафика WINS на работу сети: регистрация и возобновление имён, разрешение имён;
- Оптимизация трафика WINS;
- Захват сетевых пакетов из лабораторной сети;
- Анализ трафика регистрации имён WINS;
- Анализ трафика разрешения имён WINS;
- Выработка рекомендаций по оптимизации сетей.
- Установление соединения;
- Разрешение MAC – адреса;
- Установление сеанса связи TCP;
- Установление сеанса NETBIOS;
- Установление диалекта SMB;
- Подключение и отключение;
- Передача данных, завершение сеанса;
- Оптимизация трафика файлового сеанса связи;
- Захват пакетов из лабораторной сети;

- Анализ трафика команды NET USE;
- Анализ трафика просмотра ресурсов сервера;
- Выработка рекомендаций по оптимизации сети.

За исключением процедур разрешения имен (WINS или DNS) каждый вид обмена данных между компьютерами требует установления сеанса связи.

- Роли обозревателя;
- Настройка обозревателя;
- Составляющие трафика обзора;
- Выборы обозревателя;
- Объявления обозревателя;
- Запросы обозревателю;
- Мониторинг обозревателей;
- Влияние трафика обозревателя на работу сети;
- Получение списка обозревателя;
- Получение списка резервных обозревателей;
- Получение списка ресурсов сервера;
- Оптимизация трафика обозревателя;
- Захват пакетов из лабораторной сети;
- Анализ трафика извещений клиентов обозревателю сети;
- Анализ просмотра сетевых ресурсов клиентом;
- Составление рекомендаций по оптимизации сети.
- Алгоритмы регистрации пользователя в инфраструктуре сетевых сервисов;
- Технологии поиска серверов регистрации (контроллеров домена);
- Методы оптимизации трафика входа пользователя в систему;
- Захват пакетов из лабораторной сети;
- Определение числа контроллеров домена;
- Определение максимального количества одновременных регистраций;
- Определение оптимального места расположения к контроллеров домена;
- Определение требований к оборудованию контроллера домена;
- Проведение анализа сетевого трафика входа пользователя в систему.
- Доменная система именования хостов в сетях Internet и Intranet (DNS);
- Клиент-серверная модель и распределённая база данных DNS;
- Пространство имён доменов и домены верхнего уровня;
- Полные доменные имена, делегирование, зоны;
- Установка и настройка DNS на компьютере под управлением Windows Server;
- Настройка клиента DNS;
- Влияние трафика DNS на работу сети, транзакции DNS, запрос клиента, ответ сервера, рекурсивные транзакции DNS;
- Захват пакетов из лабораторной сети;
- Анализ трафика транзакции DNS;
- Составление рекомендаций по оптимизации сети.
- Влияние трафика просмотра интрасети на работу сети;
- Подключение к Web – узлу;
- Установление сеанса TCP для каждой страницы;
- Запрос Web – страницы;
- Защищённый доступ;

- Аутентификация по запросу;

Методические рекомендации для преподавателя

При реализации дисциплины «Сетевая безопасность» проводятся лекционные и практические занятия, а также отводится время на самостоятельную работу студентов по углубленному рассмотрению отдельных разделов дисциплины.

Лекционные занятия проводятся в виде изложения материала с использованием интерактивной доски и 2х проекторов. Лекционный курс по дисциплине построен с целью формирования у студентов ориентировочной основы для последующего усвоения материала методом самостоятельной работы. Содержание дисциплины отвечает следующим дидактическим требованиям:

- изложение материала от простого к сложному, от известного к неизвестному;
- логичность, четкость и ясность в изложении материала;
- возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студента;
- тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

Практические занятия курса проводятся по узловым и наиболее важным темам, разделам учебной программы. Они построены как на материале одной лекции, так и на содержании нескольких лекций.

При изучении дисциплины предусматривается использование интерактивных форм проведения занятий. Проводятся опросы по рассматриваемым темам. Студенты участвуют в дискуссии, задают друг другу вопросы.

Методическое обеспечение инновационных форм учебных занятий

Анализ конкретных ситуаций (CASE-STUDY) – эффективный метод активизации учебно-познавательной деятельности обучаемых. CASE – это описание реальной ситуации или «моментальный снимок реальности», «фотография действительности».

Различают несколько видов ситуаций:

- Ситуация – проблема представляет собой описание реальной проблемной ситуации. Цель обучаемых: найти решение ситуации или прийти к выводу о его невозможности.
- Ситуация – оценка описывает положение, выход из которого уже найден. Цель обучаемых: провести критический анализ принятых решений, дать мотивированное заключение по поводу представленной ситуации и её решения.
- Ситуация – иллюстрация представляет ситуацию и поясняет причины её возникновения, описывает процедуру её решения. Цель обучаемых: оценить ситуацию в целом, провести анализ ее решения, сформулировать вопросы, выразить согласие-несогласие
- Ситуация – упреждение описывает применение уже принятых ранее решений, в связи с чем ситуация носит тренировочный характер, служит иллюстрацией к той или иной теме. Цель обучаемых: проанализировать данные ситуации, найденные решения, используя при этом приобретённые теоретические знания.

Кейс может содержать описание одного события в одной организации или историю развития многих организаций за многие годы.

Требования предъявления к CASE:

- соответствовать четко поставленной цели создания;
- иметь соответствующий уровень трудности;
- иллюстрировать несколько аспектов реальной жизни;
- не устаревать слишком быстро;
- иллюстрировать типичные ситуации;
- развивать аналитическое мышление;
- провоцировать дискуссию.

В методе CASE-STUDY предполагается, что преподаватель руководит обсуждением проблемы, представленной в кейсе, а сами CASE могут быть представлены студентам в самых различных видах:

- печатном,
- видео,
- аудио,
- мультимедиа.

Методические указания для самостоятельной работы обучающихся

Самостоятельная работа студентов, предусмотренная учебным планом выполняется в ходе семестра в форме выполнения домашних заданий. Отдельные темы теоретического курса прорабатываются студентами самостоятельно в соответствии с планом самостоятельной работы и конкретными заданиями преподавателя с учетом индивидуальных особенностей студентов.

Перечень основной и дополнительной учебной литературы

Основная учебная литература

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / Олифер В.Г., Олифер Н.А. - СПб.: Питер, 2016. - ISBN 978-5-496-01967-5.
2. Алексеев Е.Б., Гордиенко В.Н., Крухмалев В.В., Моченов А.Д., Тверецкий М.С. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей: Учебное пособие для вузов -- 2-е изд., испр. - М.: Горячая линия - Телеком, 2014. - 392с.: ил. - (Учебное пособие для высших учебных заведений: Специальность). - Список лит.:с.381. - ISBN 9785991202541.
3. Лапониная, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапониная. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с. - (Основы информационных технологий). - Библиогр. в кн. ; http://biblioclub.ru/index.php?page=book_red&id=429094&sr=1
4. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз. <http://znanium.com/catalog.php?bookinfo=423927>
5. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2017. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. <https://biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7>

Дополнительная учебная литература

- 1 Таненбаум Э. Компьютерные сети. 4-е изд. — СПб.: Питер, 2002.
- 2 Крухмалев В.В. Цифровые системы передачи: Учебное пособие для вузов / Крухмалев Владимир Васильевич, Гордиенко Владимир Николаевич, Моченов Анатолий Дмитриевич; Под ред. А.Д.Моченова. - М.: Горячая линия - Телеком, 2014. - 372с.: ил. - (Учебное пособие для высших учебных заведений: Специальность). - Список лит.:с.371. - ISBN 978-5-9912-0226-8.
- 3 Куроуздж., Росс К. Компьютерные сети, 4-е изд. СПб.: Питер, 2004.
- 4 Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 572 с. : схем., ил. http://biblioclub.ru/index.php?page=book_red&id=429035&sr=1
- 5 Жуков, В. Г. Безопасность вычислительных сетей. Ч. I. Базовые протоколы стека TCP/IP [Электронный ресурс] : учеб. пособие / В. Г. Жуков. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 124 с. <http://znanium.com/catalog.php?bookinfo=463062>

• Периодические издания

- 1 Крюков Ю.А. Формирование энергоинформационной инфраструктуры на основе парадигмы интегрированной интеллектуальной распределительной сети передачи электроэнергии и данных// Энергетическая политика. – 2012. –№. 4. – С. 101-112
- 2 Сетевое научное издание «Системный анализ в науке и образовании» (свидетельство о регистрации Эл № ФС77-51141 от 14 сентября 2012 г.).
- 3 Вестник Международного университета природы, общества и человека "Дубна" / гл. ред. Е.Н. Черемисина. – Дубна: Международный университет природы, общества и человека "Дубна".- (Системный анализ в современном обществе). – Журнал.
- 4 Программные продукты и системы: научно-практическое издание. / гл. ред. С.В. Емельянов. – Тверь: МНИИПУ. – Журнал. – Международное научно-практическое приложение к журналу "Проблемы теории и практики управления".

• **Перечень ресурсов информационно-телекоммуникационной сети «Интернет»**

Электронно-библиотечные системы и базы данных научного содержания

1. Электронно-библиотечная система «Университетская библиотека онлайн»: www.bibloclub.ru
2. Электронно-библиотечная система «ЮРАЙТ» <https://biblio-online.ru>
3. Научная электронная библиотека (НЭБ): <http://elibrary.ru/defaultx.asp>
4. «Электронно-библиотечная система «Znaniy» <http://znaniy.com//>
5. БД российских журналов East View : <http://dlib.eastview.com>
6. Базы данных компании EBSCO Publishing: <http://search.ebscohost.com/>
7. БД российских научных журналов на Elibrary.ru (РУНЭБ): <http://elibrary.ru/defaultx.asp>.
8. <http://www.scopus.com/home.url>
9. Web of Science [webofknowledge.com](http://www.webofknowledge.com)

Профессиональные ресурсы сети «Интернет»

- 1 Сообщество аналитиков: <http://www.uml2.ru/>.
- 2 Материалы IT-портала Центра информационных технологий <http://www.citforum.ru>.

Перечень информационных технологий, используемых при осуществлении образовательного процесса, включая программное обеспечение, информационные справочные системы (при необходимости)

Используется лицензионное программное обеспечение:

- Wireshark Network analyzer
- MS Power Point 2012 и выше,
- Anylogic University r.7.2.
- Citrix XenApp Platinum Edition
- VMware Horizon Advanced Edition