МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ И.Е. Поверинов
31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Безопасность сетей ЭВМ»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В.Ильин
старший преподаватель С.О. Иванов

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информационных систем
«30» августа 2017г., протокол №1

заведующий кафедрой Д.В. Ильин

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета А.В. Щипцова

Директор научной библиотеки Н.Д. Никитина

Начальник управления информатизации И.П. Пивоваров

Начальник учебно-методического управления В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Целью изучения дисциплины «Безопасность сетей ЭВМ» является теоретическая и практическая подготовка обучаемых к обеспечению безопасности при эксплуатации информационно-телекоммуникационных сетей.

Основными задачами дисциплины являются:

- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Безопасность сетей ЭВМ» относится к числу дисциплин базовой части. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Безопасность операционных систем», «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем», «Управление информационной безопасностью».

Дисциплина является предшествующей для дисциплин: «Технология построения защищенных автоматизированных систем», прохождения практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

– способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);

– способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

– методы и технологии передачи данных (З1);

– виды угроз безопасности компьютерных сетей и способы защиты (З2);

уметь:

– применять программные и аппаратные средства передачи данных (У1);

– использовать методы и средства защиты информации для компьютерных сетей (У2);

владеть навыками:

– приемами настройки сети в операционных системах и в сетевых устройствах. (Н1);

– средствами обнаружения и предотвращения атак (Н2).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Архитектура сетей.	ОПК-8	З1, У1, Н1
Тема 1.1. Инфо-телекоммуникационные сети.		
Тема 1.2. Сетевые технологии.		
Тема 1.3. Основы построения сетей.		
Тема 1.4. Сетевые протоколы.		
Тема 1.5. Характеристики сетей.		
Тема 1.6. Качество обслуживания (QoS).		
Тема 1.7. Протоколы TCP/IP.		
Раздел 2. Средства сетевой защиты.	ПК-17	У2, Н2
Тема 2.1. Основные понятия сетевой безопасности.		
Тема 2.2. Сетевые экраны.		
Тема 2.3. Защита соединений.		
Тема 2.4. Системы сетевой защиты.		
Экзамен	ОПК-8, ПК-17	З1, У1, У2, Н1
Раздел 3. Уязвимости сетевых протоколов.	ОПК-8, ПК-17	З2, У2, Н1, Н2
Тема 3.1. Уязвимости стека протоколов TCP/IP.		
Тема 3.2. Физический уровень TCP/IP		
Тема 3.3. Канальный уровень TCP/IP.		
Тема 3.4.Сетевой уровень TCP/IP.		
Тема 3.5.Транспортный уровень TCP/IP.		
Тема 3.6. Уровень приложений TCP/IP.		
Экзамен	ОПК-8, ПК-17	З2, У2, Н2

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Архитектура сетей.								
Тема 1.1. Инфо-телекоммуникационные сети.	6	2	2			2	2	
Тема 1.2. Сетевые технологии.	6	2	2			2	2	
Тема 1.3. Основы построения сетей.	10	4	2			4	2	
Тема 1.4. Сетевые протоколы.	6	2	2			2	2	
Тема 1.5. Характеристики сетей.	4	2				2	2	
Тема 1.6. Качество обслуживания (QoS).	6	2	2			2	2	
Тема 1.7. Протоколы TCP/IP.	10	2	6			2	2	
Раздел 2. Средства сетевой защиты.								
Тема 2.1. Основные понятия сетевой безопасности.	15	4		8		3	2	
Тема 2.2. Сетевые экраны.	15	4		8		3	2	
Тема 2.3. Защита соединений.	15	4		8		3	2	
Тема 2.4. Системы сетевой защиты.	15	4		8		3	2	
Экзамен	36							36
Раздел 3. Уязвимости сетевых протоколов.								

Тема 3.1. Уязвимости стека протоколов TCP/IP.	11	4	2	2		3	2	
Тема 3.2. Физический уровень TCP/IP	19	2	6	6		5	2	
Тема 3.3. Канальный уровень TCP/IP.	19	2	6	6		5	2	
Тема 3.4.Сетевой уровень TCP/IP.	19	2	6	6		5	2	
Тема 3.5.Транспортный уровень TCP/IP.	18	2	6	6		4	2	
Тема 3.6. Уровень приложений TCP/IP.	20	4	6	6		4	2	
Экзамен	36				2			36
Итого	**288 8 з.е.**	**48**	**48**	**64**	**2**	**54**	**34**	**72**

5. Содержание разделов дисциплины

5.1. Лекции

Раздел 1. Архитектура сетей.

Тема 1.1. Инфо-телекоммуникационные сети.

Лекция 1. Инфо-телекоммуникационные сети.

1. Особенности инфо-телекомуникационной связи.
2. Виды и характеристики сетей. Терминология.
3. Основные концепции современных сетей.

Тема 1.2. Сетевые технологии.

Лекция 2. Сетевые технологии.

1. Сетевое оборудование.
2. Сетевое ПО.
3. Стандартизация сетей.

Тема 1.3. Основы построения сетей.

Лекция 3. Принципы построения сетей.

1. Идеальная сеть. Проблемы и принципы построения сетей.
2. Трансляция. Кодирование, модуляция, мультиплексирование сигналов.
3. Топология. Виды связей между узлами. Базовые топологии.

Лекция 4. Коммутация и маршрутизация.

1. Адресация. Адресное пространство. Виды адресов.
2. Коммутация. Принципы коммутации. Достоинства и недостатки различных видов коммутации.
3. Маршрутизация. Принципы маршрутизации.

Тема 1.4. Сетевые протоколы.

Лекция 5. Сетевые протоколы.

1. Стек протоколов.
2. Сетевые модели.
3. Классификация сетевого оборудования по уровням модели OSI.

Тема 1.5. Характеристики сетей.

Лекция 6. Характеристики сетей.

1. Понятие метрики.
2. Метрики производительности.
3. Метрики надежности.

Тема 1.6. Качество обслуживания (QoS).

Лекция 7. Качество обслуживания (QoS).

1. Перегрузка (congestion).
2. Способы управления качеством обслуживания.

Тема 1.7. Протоколы TCP/IP.

Лекция 8. Протоколы TCP/IP.

1. Технологии передачи сигналов.
2. Протоколы канального уровня
3. Протоколы сетевого уровня
4. Протоколы транспортного уровня

5. Протоколы уровня приложений.

Раздел 2. Средства сетевой защиты

Тема 2.1. Принципы сетевой безопасности.

Лекция 9. Проблемы сетевой безопасности.

1. Проблемы и уязвимости сетевых протоколов.
2. Виды сетевых атак.

Практическое занятие 1.1. Сетевой полигон.

Лекция 10. Пентестинг.

1. Принцип работы генераторов трафика.
2. Принцип работы перезватчиков трафика.
3. Инструменты генерации, перехвата и анализа сетевых пакетов.

Практическое занятие 1.2. Скрытый канал.

Тема 2.2. Сетевые экраны.

Лекция 11. Сетевые экраны.

1. Принцип работы.
2. Классификация сетевых экранов.
3. Демилитаризованная зона.

Практическое занятие 1.3. Iptables.

Лекция 12. Демилитаризованная зона (DMZ).

1. Концепция и назначение DMZ.
2. Архитектура и особенности реализации DMZ.

Практическое занятие 1.4. DMZ.

Тема 2.3. Защита соединений.

Лекция 13. Удаленный доступ.

1. Средства и протоколы удаленного доступа и туннелирования.
2. Протокол SSH.

Практическое занятие 1.5. SSH.

Лекция 14. Криптошлюзы.

1. Функции и принцип работы.
2. Криптошлюз Континент-М.

Практическое занятие 1.6. Криптошлюз.

Тема 2.4. Системы сетевой защиты.

Лекция 15. Системы обнаружения и предотвращения вторжений.

1. Принцип работы систем обнаружения и предотвращения вторжений.
2. Применение системы обнаружения и предотвращения вторжений.

Практическое занятие 1.7. IDS/IPS.

Лекция 16. Средства заманивания и отвлечения злоумышленников.

1. Принцип работы средств заманивания и отвлечения злоумышленников.
2. Применение средств заманивания и отвлечения злоумышленников.

Практическое занятие 1.8. Honeypot.

Раздел 3. Уязвимости сетевых протоколов.

Тема 3.1. Уязвимости стека протоколов TCP/IP.

Лекция 1. Основы сетевой безопасности.

1. Виды сетевых атак на различных уровнях модели TCP/IP.
2. Средства сетевой защиты.

Лекция 2. Уязвимости стека протоколов TCP/IP.

1. Технология Ethernet.
2. Стек протоколов TCP/IP.
3. Классификация уязвимостей протоколов TCP/IP по уровням OSI.

Практическое занятие 2.1. Инструменты пентестера.

Тема 3.2. Физический уровень TCP/IP

Лекция 3. Физическая защита линии связи.

1. Уязвимости проводных/беспроводных сред передачи сигналов.
2. Нарушение КЦД информации передаваемой по линиям связи.
3. Средства физической защиты целостности канала.
4. Обеспечение надежной связи между узлами.
5. Обнаружение нелегального подключения.

Практическое занятие 2.2. Подключение к витой паре.
Практическое занятие 2.3. Подключение к wifi-сети.
Практическое занятие 2.4. Обнаружение и блокирование подключений.

Тема 3.3. Канальный уровень TCP/IP.

Лекция 4. Защита каналов передачи.

1. Уязвимости протоколов канального уровня.
2. Прослушивание трафика.
3. Вмешательство в трафик.
4. Обнаружение снифферов в сети.
5. Ограничение доступа в сеть и обнаружение подозрительной деятельности.
6. Аутентификация и контроль доступа в сеть(802.1x).

Практическое занятие 2.5. Определение сетевых настроек.
Практическое занятие 2.6. Атака сниффинг трафика.
Практическое занятие 2.7. Обнаружение снифферов.

Тема 3.4.Сетевой уровень TCP/IP.

Лекция 5. Защита механизмов адресации и маршрутизации.

1. Уязвимости протоколов сетевого уровня.
2. Нарушение адресации и маршрутизации.
3. Проблема «человек посередине».
4. Настройка сетевой политики.
5. Межсетевые экраны.
6. Протокол IPv6.

Практическое занятие 2.8. Настройка IPv6-сети.
Практическое занятие 2.9. Атака подмена IP-адреса.
Практическое занятие 2.10. Защита протокола ICMP.

Тема 3.5.Транспортный уровень TCP/IP.

Лекция 6. Защита транспортных потоков.

1. Уязвимости протоколов транспортного уровня.
2. Нарушение последовательности.
3. Перехват и вмешательство в передаваемые данные.
4. Ограничение соединений.
5. Шифрование и туннелирование.
6. Инфраструктура открытых ключей.

Практическое занятие 2.11. Сканирование портов.
Практическое занятие 2.12. Атака ssl-strip.
Практическое занятие 2.13. Атака SYN-flood.

Тема 3.6. Уровень приложений TCP/IP.

Лекция 7. Защита сетевых ресурсов.

1. Атаки на сетевые сервисы.
2. Отказ в обслуживании (DOS, DDOS).
3. Уязвимости сетевых приложений.
4. Проксирование и защита от атак отказа в обслуживании.
5. Анализ защищенности сетевых ресурсов.
6. Обнаружение сетевых атак. Заманивание и отвлечение злоумышленников.

Практическое занятие 2.14. Инвентаризация уязвимостей.
Практическое занятие 2.15. Эксплуатация уязвимостей протоколов.
Практическое занятие 2.16. Атака DOS.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторное занятие 1.1. Анализ сети.	2
Лабораторное занятие 1.2. Подключение к сети.	2
Лабораторное занятие 1.3. Настройка сети.	2
Лабораторное занятие 1.4. Использование сети.	2
Лабораторное занятие 1.5. Отладка сети.	2
Лабораторное занятие 1.6. Симулятор сети GNS3.	6
Лабораторное занятие 2.1. Инструменты пентестера.	2
Лабораторное занятие 2.2. Подключение к витой паре.	2
Лабораторное занятие 2.3. Подключение к wifi-сети.	2
Лабораторное занятие 2.4. Обнаружение и блокирование подключений.	2
Лабораторное занятие 2.5. Определение сетевых настроек.	2
Лабораторное занятие 2.6. Атака сниффинг трафика.	2
Лабораторное занятие 2.7. Обнаружение снифферов.	2
Лабораторное занятие 2.8. Настройка IPv6-сети.	2
Лабораторное занятие 2.9. Атака подмена IP-адреса.	2
Лабораторное занятие 2.10. Защита протокола ICMP.	2
Лабораторное занятие 2.11. Сканирование портов.	2
Лабораторное занятие 2.12. Атака ssl-strip.	2
Лабораторное занятие 2.13. Атака SYN-flood.	2
Лабораторное занятие 2.14. Инвентаризация уязвимостей.	2
Лабораторное занятие 2.15. Эксплуатация уязвимостей протоколов.	2
Лабораторное занятие 2.16. Атака DOS.	2
Итого	48

5.3. Вопросы для самостоятельной работы студента

Раздел 1. Архитектура сетей.

1. Построение схемы и карты сети.
2. Установка драйверов сетевых устройств.
3. Создание виртуальных сетевых устройств.
4. Симулятор сети GNS3.

Раздел 2. Средства сетевой защиты.

1. Тунелирование и шифрование сетевого трафика с помощью SSH.
2. Защита локальной сети с помощью NAT.
3. Установка и настройка VPN-сервера.

Раздел 3. Уязвимости сетевых протоколов.

1. Затруднение доступа к линиям связи и усложнение подключения к ним.
2. Перехват информации с помощью анализатора сетевого трафика.
3. Протоколы сетевой аутентификации
4. Сбор информации о сетевом окружении
5. Осуществление атак отказа в обслуживании.
6. Методы обнаружения снифферов.
7. Настройка сетевого экрана iptables. Блокирование сетевых атак

8. Атаки типа man-in-middle
9. Протоколы и средства шифрования и сжатия трафика.
10. Сетевая аутентификации по протоколу RADIUS/TACAS.
11. Средства защиты беспроводных сетей.
12. Сетевые полигоны для тестирования средства и методов сетевой защиты.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.).

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;

– практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

– лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: составление вопросов и тестов к теме, подготовка к лабораторным работам, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на экзамене.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме экзаменов. Принимаются экзамены преподавателями, читающими лекции по данной учебной дисциплине в соответствии с

перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к экзаменам

Семестр 8.

1. Компьютерная (инфокоммуникационная) сеть. Эволюция сетей. Виды. Характеристики.
2. Сетевые технологии: сетевое оборудование, сетевое ПО, сетевые стандарты.
3. Архитектура и принципы построения сетей. Основные понятия. Топология. Адресация.
4. Коммутация. Виды. Преимущества и недостатки.
5. Стек протоколов. Сетевые модели. Классификация сетевого оборудования по сетевым уровням.
6. Связь между пропускной способностью и перегрузками, и заторами. Измерение характеристик сети. Метрики.
7. Классы QoS. Методы обеспечения качества обслуживания.
8. Физический уровень сети. Элементы спектральной теории сигналов. Согласование характеристик каналов связи и сигналов
9. Физический уровень сети. Особенности различных каналов связи.
10. Физический уровень сети. Модуляция сигналов.
11. Физический уровень сети. Мультиплексирование сигналов.
12. Канальный уровень. Фрейм. Формирование фрейма. Обнаружение проблем.
13. Канальный уровень. Устранение ошибок.
14. Канальный уровень. Разделяемая среда. Коллизии. Протоколы коллективного доступа
15. Канальный уровень. Объединение и разделение сегментов. Принцип работы коммутатора. Виртуальные сети.
16. Сетевой уровень. Маршрутизация: принципы, характеристики и виды алгоритмов. Метрики длин путей. Алгоритмы маршрутизации.
17. Сетевой уровень. Транзит пакетов: виды, особенности, способы. Принцип работы маршрутизатора
18. Сетевой уровень. Балансировка нагрузки. Ограничения и особенности данного уровня.
19. Сетевой уровень. Объединение сетей. Магистрали. Туннелирование. Преобразование адресов. Фрагментирование.
20. Транспортный уровень. Сетевые службы и порты. Сокеты.
21. Транспортный уровень. Транспортный протокол. Особенности подключения, разрыва, отправки и получения данных.
22. Транспортный уровень. Контроль ошибок. Восстановление соединения.
23. Транспортный уровень. Контроль перегрузок.
24. Уровень приложений. Клиент-серверная и распределенная модели. Сетевые службы и сервисы.
25. World Wide WEB. Принципы организации и работы.
26. Классификация сетевых атак.
27. Классификация протоколов TCP/IP.
28. Архитектура системы обеспечения сетевой безопасности.
29. Системный подход к сетевой безопасности.
30. Виртуальные сети: назначение, виды, достоинства и недостатки.
31. Программное и аппаратное обеспечение виртуальных сетей.
32. Стандарт виртуальных сетей IEEE 802.1q.
33. Настройка виртуальной сети по стандарту IEEE 802.1q.
34. Сетевая аутентификация: принципы, проблемы.
35. Программное и аппаратное обеспечение сетевой аутентификации.

36. Настройка сетевой аутентификации по протоколу Kerberos.
37. Архитектура системы сетевой аутентификации по протоколу Kerberos.
38. Сетевые экраны: виды, принцип работы.
39. Программные и аппаратные сетевые экраны.
40. Архитектура сетевого экрана Netfilter.
41. Настройка сетевого экран Netfilter.
42. Удаленный доступ: назначение, виды, принципы защиты.
43. Программное и аппаратное обеспечение удаленного доступа.
44. Архитектура сервера OpenSSH.
45. Настройка удаленного доступа по протоколу SSH.
46. Криптошлюзы: функции и возможности, устройство, принцип работы.
47. Программные и аппаратные криптошлюзы.
48. Криптошлюз Континент-М: характеристики, возможности.
49. Настройки политики безопасности на криптошлюзах.
50. Система обнаружения и предотвращения вторжения по сети: цели и задачи, критерии обнаружения, принцип работы.
51. Программные и аппаратные системы обнаружения и предотвращения вторжений по сети.
52. Архитектура системы обнаружения и предотвращения вторжений по сети Snort.
53. Настройка системы обнаружения и предотвращения вторжений по сети Snort.
54. Система заманивания и отвлечения злоумышленников в сети: цели и задачи, виды, принцип работы.
55. Программные и аппаратные системы заманивания и отвлечения злоумышленников в сети.
56. Архитектура системы заманивания и отвлечения злоумышленников в сети Honeyd.
57. Настройка системы заманивания и отвлечения злоумышленников в сети Honeyd.
58. Подключиться к сети
59. Настроить сеть.
60. Получить билет по сети.
61. Построить схему сети.
62. Передать файл с ответом на практическое задание по ftp.
63. Настроить подключение по SSH по ключу.
64. Настроить блокирование любого входящего трафика.

Семестр 9.

1. Классификация сетевых атак.
2. Архитектура системы обеспечения сетевой безопасности.
3. Виртуальные сети: назначение, виды, достоинства и недостатки.
4. Программное и аппаратное обеспечение виртуальных сетей.
5. Настройка виртуальной сети по стандарту IEEE 802.1q.
6. Сетевая аутентификация: принципы, проблемы.
7. Программное и аппаратное обеспечение сетевой аутентификации.
8. Настройка сетевой аутентификации по протоколу Kerberos.
9. Сетевые экраны: виды, принцип работы.
10. Программные и аппаратные сетевые экраны.
11. Настройка сетевого экран Netfilter.
12. Удаленный доступ: назначение, виды, принципы защиты.
13. Программное и аппаратное обеспечение удаленного доступа.
14. Настройка удаленного доступа по протоколу SSH.
15. Криптошлюзы: функции и возможности, устройство, принцип работы.
16. Программные и аппаратные криптошлюзы.
17. Настройки политики безопасности на криптошлюзах.

18. Система обнаружения и предотвращения вторжения по сети: цели и задачи, критерии обнаружения, принцип работы.
19. Программные и аппаратные системы обнаружения и предотвращения вторжений по сети.
20. Настройка системы обнаружения и предотвращения вторжений по сети Snort.
21. Система заманивания и отвлечения злоумышленников в сети: цели и задачи, виды, принцип работы.
22. Программные и аппаратные системы заманивания и отвлечения злоумышленников в сети.
23. Настройка системы заманивания и отвлечения злоумышленников в сети Honeyd.
24. Сети TCP/IP: структура, используемые технологии.
25. Классификация протоколов TCP/IP по уровням OSI.
26. Основные протоколы TCP/IP.
27. Среды передачи сигналов: виды, характеристики, достоинства и недостатки.
28. Сетевое оборудование: виды, характеристики, достоинства и недостатки.
29. Уязвимости сред передачи сигналов.
30. Способы атак на линии связи на физическом уровне.
31. Способы обеспечения надежной связи между узлами.
32. Средства физической защиты линий связи.
33. Способы обнаружение проблем с линией связи.
34. Протоколы канального уровня: виды, назначение.
35. Принцип работы протоколов канального уровня.
36. Уязвимости протоколов канального уровня
37. Подключение и прослушивание трафика на канальном уровне.
38. Ограничение и фильтрация доступа к сети
39. Обнаружение снифферов и подозрительной активности.
40. Стандарты сетевой аутентификации IEEE 802.1x
41. Протоколы сетевого уровня: виды, назначение.
42. Принцип работы протоколов сетевого уровня.
43. Уязвимости протоколов сетевого уровня.
44. Проблема "man-in-middle".
45. Обеспечение правильности маршрутизации.
46. Настройка сетевой политики ОС.
47. Возможности протокола IPv6.
48. Протоколы транспортного уровня: виды, назначение.
49. Принцип работы протоколов транспортного уровня.
50. Уязвимости протоколов транспортного уровня.
51. Сканирование портов: цели, возможности, способы защиты
52. Виртуальные частные сети: назначение, возможности, принцип работы.
53. Защищенные транспортные протоколы: назначение, возможности, принцип работы.
54. Инфраструктура открытых ключей: назначение, архитектура, принцип работы.
55. Протоколы приложений: виды, назначение.
56. Принципы работы протоколов приложений.
57. Уязвимости сетевых приложений.
58. Инъекции кода и удаленный запуск кода.
59. Списки уязвимостей: цели и задачи, принципы составления, виды.
60. Отказ в обслуживании: принципы осуществления, способы защиты.
61. Прокси-сервера: назначение, виды, принцип работы.
62. Спам: определение, способы борьбы.
63. Боты и ботсети: виды, принцип работы, способы защиты.
64. Бэкдоры (backdoor): виды, принцип работы, способы защиты.

7.2. Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Эндрю Таненбаум. Уэзеролл. Компьютерные сети // Классика Computer Science. - 2012. - 960 с.
2.	Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс] : учебное пособие / БехроузА. Фороузан. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 782 c. — 978-5-4487-0143-6. — Режим доступа: http://www.iprbookshop.ru/72337.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Криптография и безопасность цифровых систем [Электронный ресурс] : учебное пособие / В.Г. Грибунин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 c. — 978-5-9515-0166-0. — Режим доступа: http://www.iprbookshop.ru/60851.html
2.	Голиков А.М. Кодирование в телекоммуникационных системах [Электронный ресурс] : учебное пособие для специалитета: 090302.65 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, задание на самостоятельную работу / А.М. Голиков. — Электрон. текстовые данные. — Томск: Томский государственный университет систем управления и радиоэлектроники, 2016. — 338 c. Режим доступа: http://www.iprbookshop.ru/72111.html

Нормативные правовые и методические документы в области защиты информации доступны по ссылке https://fstec.ru/component/tags/tag/informatsionnoe-soobshchenie

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Windows/Tinycore linux	лицензия университета/ свободное лицензионное соглашение (http://tinycorelinux.net/downloads.html)
2.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Виртуальная машина Virtualbox	свободное лицензионное соглашение на ПО: GNU GPL (https://www.virtualbox.org/wiki/Downloads)
4.	Эмулятор сетевого оборудования	Свободное лицензионное соглашение на ПО: GNU GPL (http://www.gns3.com/)

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Xgu.ru.	http://xgu.ru/wiki/
2.	Российская Государственная Библиотека	http://www.rsl.ru
3.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
4.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
5.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
6.	Научная электронная библиотека	http://elibrary.ru
7.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
8.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением;

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу

обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

Для реализации программы обучения используется лаборатория оснащённая:

- коммутаторами (DES-1008A – 5);
- маршрутизаторами (Wifi-роутер TP-LINK TL-WR841N - 1);
- межсетевыми экранами (D-Link <DFL-260E>NETDEFEND Firewall (5UTP 10/100/1000Mbps) - 2);
- анализаторами кабельных сетей (Network LAN Cable Tester - RJ45, RJ11, RJ12, CAT5, UTP);
- системы защиты от утечки данных (Аппаратно-программным комплексом шифрования (АПКШ) ЦУС Платформа IPC-25(4порта) - 2).

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-

конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.

Лист актуализации

№ п/п	Наименование документа	Решение кафедры		Подпись	Должность, ФИО
		Дата	протокол №		