МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) Безопасность автоматизированных систем

(по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования: бакалавриат
Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2022*

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ
Рабочая программа дисциплины

Составитель:
Кандидат технических наук, доцент кафедры КЗИ А.С. Моляков

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 31.03.2022

Оглавление

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины: приобретение знаний о базовых методах и способах защиты сетевых технологий и умений применять на практике средства защиты сетевых протоколов, в том числе стека протоколов TCP/IP.

Задачи дисциплины: изучение принципов сетевого взаимодействия; выработка умений настраивать и применять средства сетевого взаимодействия, использовать инструменты настройки сетевой инфраструктуры, в том числе на базе стека протоколов TCP/IP.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-4.3 Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 Знает требования по установке, настройке, администрированию и обслуживанию программно-аппаратных и технических средств защиты информации автоматизированных систем	Знать: требования по установке, настройке, администрированию и обслуживанию систем защиты информации в вычислительных сетях на примере МЭ, СОВ, сканеров уязвимостей.
	ОПК-4.3.2 Умеет настраивать программное обеспечение системы защиты информации, выявлять и анализировать уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации	Уметь: настраивать системы защиты информации в вычислительных сетях на примере МЭ, СОВ, сканеров уязвимостей.
	ОПК-4.3.3 Владеет навыками по осуществлению планирования и организации работы персонала автоматизированной системы с учетом требований по защите информации	Владеть: навыками по осуществлению планирования и организации работы персонала вычислительных сетей с учетом требований по защите информации.
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	Знать: математические модели кодирования систем информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
	ОПК-9.2 Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации	Уметь: применять теоретические знания при разработке ОРД; применять информационные технологии для поиска и обработки информации; применять математические модели для оценки защищенности вычислительных сетей
	ОПК-9.3 Владеет методами и средствами крипто-	Владеть: навыками поиска нужной информации в нормативных базах и ис-

	графической и технической защиты информации	точниках; навыками эксплуатации криптографических протоколов и схем в вычислительных сетях

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Безопасность вычислительных сетей» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: «Сети и системы передачи данных», «Информационные технологии».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практик: «Защита информации от вредоносного программного обеспечения», «Информационная безопасность телекоммуникационных систем», «Безопасность операционных систем», «Преддипломная практика».

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часов

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**24**
7	Практические занятия	**36**
Всего:		**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _48_ академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Введение в теорию и практику обеспечения безопасности сетевых технологий**	Сеть. Общие понятие. Обзор существующих сетевых топологий.
2	**Базовая эталонная модель OSI/ISO. Архитектура защиты информации**	Описание базовой эталонной модели OSI/ISO. 7 уровней функционирования. Архитектурные принципы реализации защищенных сетевых взаимодействий.
3	**Стек протоколов TCP/IP. Канальный, сетевой (межсетевой), транспортный и прикладной уровни**	Стек протоколов TCP/IP. Поля и флаги пакетов. Применение 4 уровней при разработке средств защиты информации. Особенности семейства протоколов TCP/IP и сетей на его основе. Стек протоколов TCP/IP включает в себя: • IP (Internet Protocol) – межсетевой протокол, который обеспечивает транспортировку без дополнительной обработки данных с одной машины на другую;

		• UDP (User Datagram Protocol) – протокол пользовательских датаграмм, обеспечивающий транспортировку отдельных сообщений с помощью IP без проверки ошибок; • TCP (Transmission Control Protocol) – протокол управления передачей, обеспечивающий транспортировку с помощью IP с проверкой установления соединения; • ICMP (Internet Control Message Protocol) – межсетевой протокол управления сообщениями, который отвечает за различные виды низкоуровневой поддержки протокола IP, включая сообщения об ошибках, содействие в маршрутизации, подтверждение в получении сообщения; • ARP (Address Resolution Protocol) – протокол преобразования адресов, выполняющий трансляцию логических сетевых адресов в аппаратные;
4	**Реализация протоколов стека TCP/IP, протоколы Ethernet, IP, TCP, UDP. HTTP, FTP и другие**	Примеры реализация протоколов стека TCP/IP, использование сетевых протоколов в современных программно-аппаратных решений.
5	**Угрозы, атаки и уязвимости в сетях на базе TCP/IP, методы и механизмы защиты от них**	Современные угрозы в сетях на базе TCP/IP. • Проблемы с системами шифрования и цифровой подписи – возможна некорректная обработка даты создания обрабатываемых сообщений. • Ошибки в работе систем электронной коммерции, систем электронных торгов и резервирования заказов – неправильная обработка даты. • Проблемы с модулями автоматизированного контроля безопасности системы и протоколирования событий – неправильное ведение журнала и его анализ. • Проблемы с модулями реализации авторизованного доступа к ресурсам системы – невозможность доступа к системе в определённые даты. • Проблемы с запуском в определённое время модулей автоматического анализа безопасности системы и поиска вирусов. • Проблемы с системами защиты от нелегального копирования, основанными на временных лицензиях. • Проблемы с работой операционных систем. • Неправильная обработка даты аппаратными средствами защиты. Методы защиты от удалённых атак в сети Internet. Наиболее простыми и дешёвыми являются административные методы защиты, как то использование в сети стойкой криптографии, статических ARP-таблиц, hosts файлов вместо выделенных DNS-серверов, использование или неиспользование определённых операционных систем и другие методы. Следующая группа методов защиты от удалённых атак – программно-аппаратные. К ним относятся: • программно-аппаратные шифраторы сетевого трафика; • методика Firewall; • защищённые сетевые криптопротоколы; • программные средства обнаружения атак (IDS – Intrusion Detection Systems или ICE – Intrusion Countermeasures Electronics); • программные средства анализа защищённости

		(SATAN – Security Analysis Network Tool for Administrator, SAINT, SAFEsuite, RealSecure и др.).
6	**Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых протоколов**	ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Введение в теорию и практику обеспечения безопасности сетевых технологий	Лекция 1.1 Лекция 1.2 Практическое занятие 1. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Изучение материалов лекций
2	Базовая эталонная модель OSI/ISO. Архитектура защиты информации.	Лекция 2.1 Лекция 2.2 Самостоятельная работа	Традиционная с использованием презентаций Тестирование Изучение материалов лекций
3	Стек протоколов TCP/IP. Канальный, сетевой (межсетевой), транспортный и прикладной уровни	Лекция 3.1 Лекция 3.2 Практическое занятие 2. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций
4	Реализация протоколов стека TCP/IP, протоколы Ethernet, IP, TCP, UDP. HTTP, FTP и другие	Лекция 4.1 Лекция 4.2 Практическое занятие 3. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций
5	Угрозы, атаки и уязвимости в сетях на базе TCP/IP, методы и механизмы защиты от них	Лекция 5.1 Лекция 5.2 Практические занятие 4. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания Изучение материалов лекций
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых протоколов	Лекция 6.1 Лекция 6.2 Практическое занятие 5. Самостоятельная работа	Традиционная с использованием презентаций Тестирование Выполнение задания. Специализированное ПО - VPN-клиенты: ZPN-Connet, Free VPN, OpenVPN, VPN Monster, Whoer VPN, Windscribe VPN, сниффер WireShark Изучение материалов лекций

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - *Тестирование (темы 1-6)* - *практические занятия (темы 1-3)* - *практические занятия (темы 4-6)*	*5 баллов* *6 баллов* *8 баллов*	*30 баллов* *6 баллов* *24 балла*
Промежуточная аттестация – э*кзамен* *(экзамен по билетам)*		*40 баллов*
Итого за семестр		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	Темы 1 – 6	ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3	Опрос
2.	Практические занятия 1 – 5	ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3	План практического занятия

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2.Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Контрольные вопросы к экзамену - *проверка сформированности компетенций ОПК-9, ОПК-4.3*

Контрольные вопросы	Реализуемые компетенции
1. Архитектура компьютерных сетей.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
2. Модель OSI/ISO. Уровни взаимодействия в рамках компьютерных сетей. Понятие протоколов и интерфейсов.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
3. Стек протоколов TCP/IP. Процедура инкапсуляции.	ОПК-9.1, ОПК-9.2,ОПК-

	9.3
4. Физический и канальные уровни модели OSI/ISO. Топология сетей. Коммуникационное оборудование канального уровня.	ОПК-9.1, ОПК-9.2,ОПК-9.3
5. Формат кадра Ethernet. Технология CSMA/CD.	ОПК-9.1, ОПК-9.2,ОПК-9.3
6. Принципы построения сетей, сегментированных на канальном уровне.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
7. Назначение и принципы работы протоколов ARP/RARP. Атака ARP-spoofing.	ОПК-9.1, ОПК-9.2,ОПК-9.3
8. Функции и принципы реализации протокола IP. Формат заголовка IP.	ОПК-9.1, ОПК-9.2,ОПК-9.3
9. Фрагментирование IP пакетов. MTU.	ОПК-9.1, ОПК-9.2,ОПК-9.3
10. Настройка сетевого интерфейса в ОС Microsoft и Unix. Статическая маршрутизация.	ОПК-9.1, ОПК-9.2,ОПК-9.3
11. Настройка статической маршрутизации на примере оборудования Cisco.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
12. Протоколы динамической маршрутизации.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
13. Протоколы управления сетью на примере ICMP и SNMP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
14. Функции и принципы работы протоколов транспортного уровня. Заголовки протоколов TCP и UDP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
15. Системы пакетной фильтрации на примере ipfw.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
16. Назначение и принципы работы протокола DNS.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
17. Назначение и принципы работы протокола FTP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
18. Протокол HTTP, настройка HTTP-сервера на примере apache и nginx.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
19. Протоколы почтовой связи на примере POP2(IMAP) и SMTP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
20.Организация защищенного канала связи с использованием протокола SSL/TLS.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
21. DNS-туннелирование. Использование данной технологии для обхода межсетевых экранов.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
22. XSS-атаки на сайты.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3

23. Понятие фишинга.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3
24. Утилиты nmap и hping3 для зондирования сетей.	ОПК-9.1, ОПК-9.2,ОПК-9.3, ОПК-4.3.1;ОПК-4.3.2, ОПК-4.3.3

Примерные задания для тестирования - *проверка сформированности компетенций ОПК-9, ОПК-4.3*

1. DNS-туннелирование - это:
а) техника, позволяющая передавать произвольный трафик (фактически, поднять туннель) поверх DNS-протокола. Может применяться, например, для того чтобы получить полноценный доступ к Интернет из точки, где разрешено преобразование DNS-имён
б) SSL-соединение.
в) криптошлюз.

2. MAC-спуффинг – это:
а) стек сетевого устройства.
б)подделивание MAC-адреса сетевого устройства.
в) HTTP запрос.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

1. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.
2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

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. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450234
2. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020.

— 333 с. — (Высшее образование). — ISBN 978-5-9916-9956-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452430

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для вузов / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 351 с. — (Высшее образование). — ISBN 978-5-9916-9958-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453063
4. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285
5. *Комплексная защита* информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
6. *Шаньгин В.Ф.* Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В. Ф. Шаньгин. - М.: ДМК Пресс, 2010. - 544 с.: ил. - ISBN 978-5-94074-518-1. - Режим доступа: http://znanium.com/catalog/product/408107

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Гарант [Электронный ресурс]: информационно-правовой портал. – Электрон. дан. – М.: НПП "ГАРАНТ-СЕРВИС", 2018. – Режим доступа: www.garant.ru.

2. Консультант Плюс [Электронный ресурс]. – Электрон. дан. – М.: Консультант Плюс, cop. 1997-2018. – Режим доступа: www.consultant.ru.

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru
Cambridge University Press
ProQuest Dissertation & Theses Global
SAGE Journals
Taylor and Francis
JSTOR

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office

3. Kaspersky Endpoint Security

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Microsoft Share Point 2010
6. Secret Net Studio 8.4
7. Dallas Lock 8.0
8. Vmware Player 15.5
9. XSpider 7.0
10. Nmap 7.8
11. Wireshark 3.0
12. ZPN-Connet
13. Free VPN
14. VPN Monster
15. Whoer VPN
16. Windscribe VPN

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа;

– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;

– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;

– в форме электронного документа;

– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;

– дисплеем Брайля PAC Mate 20;

– принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;

– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

- *проверка сформированности компетенций ОПК-9, ОПК-4.3*

Темы учебной дисциплины предусматривают проведение практических(семинарских) занятий, которые служат как целям текущего и промежуточного контроля за подготовкой студентов, так и целям получения практических навыков применения методов выработки реше-

ний, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения.

Практическое занятие 1(8 ч.). Изучение сетей Ethernet и Infiniband- *проверка сформированности компетенций ОПК-9, ОПК-4.3*

*Вопросы для обсуждения***:**

1. Стандарт 801.2. Работа с Ethernet-кадрами.
2. Что такое Infiniband.
3. Сравнить Ethernet и Infiniband.
4. Пакет управления MLNX IB.
5. 400G Ethernet — новейший стандарт для высокоскоростных оптических интерфейсов. Первоначально известный как IEEE 802.3bs, 400 Gigabit Ethernet был официально утвержден в декабре 2017 года и является частью более широкого семейства технологий, таких как 200G, а также следующего поколения 100G и 50G Ethernet.
6. Технология плотного мультиплексирования с разделением по длине волны (Dense Wavelength Division Multiplexing, DWDM).

Практическое занятие 2(8 ч.). Нормативно-методическая база использования. Краткий обзор руководящих документов - *проверка сформированности компетенций ОПК-9, ОПК-4.3*

Вопросы для обсуждения:

1.Перечень основных нормативно-правовых документов.

2. Понятие сеть TCP/IP.

3. Топология сетей.

Практическое занятие 3(4 ч.). Модель OSI. Структура пакетов IP - *проверка сформированности компетенций ОПК-9, ОПК-4.3*

Вопросы для обсуждения:

1.Понятие модель OSI.

2. Назовите уровни функционирования согласно модели OSI.

3. Основные флаги пакетов IP. Структура заголовков.

4. На каком уровне работает протокол icmp.

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия: аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук). Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной VMPlayer, сниффер WireShark.

Практическое занятие 4(8 ч.). Угрозы, атаки и уязвимости в сетях на базе TCP/IP - *проверка сформированности компетенций ОПК-9, ОПК-4.3*

Вопросы для обсуждения:

1.Понятие угрозы.

2. Назовите три средства обнаружения атак.

3. Какие атаки вы знаете ? Покажите на наглядном примере схему реализации атаки.

4. Какие уязвимости эксплуатируют злоумышленники для реализации атак?

Практическое занятие 5(8 ч.). Обычный и каскадный VPN - проверка сформированности компетенций ОПК-9, *ОПК-4.3*

Порядок выполнения сертификационных исследований

1. Установить и настроить VPN клиент на хост е
2. Убедиться в работоспособности сети.
3. Рабочие конфигурация для выполнения сертификационных исследований:

- Когда VPN поднят только на хосте.
- Когда VPN запущен и в ВМ, и запущен на хосте
- Когда нет VPN ни на хосте, ни в гостевой ОС

Открыть Web-браузер и воспользоваться сервисами https://whatismyipaddress.com/
https://www.myip.com/
https://whoer.net/
https://iplocation.com/

Убедиться, что после VPN-подключени я IP адрес, определяемый Интернет- сервисами поменялся.

4. Тестирование на утечки (анонимный серфинг) обычный и каскадный VPN. Зайти на следующие зарубежные сайт ы и запустить проверки … Результаты добавить в лабораторный от чет:

https://ipleak.net/
https://www.perfect-privacy.com/check-ip
https://ipx.ac/run
https://browserleaks.com/webrtc
https://www.perfect-privacy.com/dns-leaktest/
https://dnsleak.com

5. Можете запустить дополнительные тесты (дополнительные режимы проверки) : https://browserleaks.com/proxy

https://browserleaks.com/ip
https://browserleaks.com/javascript
https://browserleaks.com/features
https://browserleaks.com/webgl

Дополнительные сайты для тестирования:
https://www.dnsleaktest.com/
https://www.astrill.com/vpn-leak-test

6. Затем зайти на отечественный сайт https://2ip.ru/privacy/. Провести проверку и представить отчет.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Безопасность вычислительных сетей» реализуется на факультете Информационных систем и безопасности кафедрой комплексной защиты информации.

Цель дисциплины: приобретение знаний о базовых методах и способах защиты сетевых технологий и умений применять на практике средства защиты сетевых протоколов, в том числе стека протоколов TCP/IP.

Задачи дисциплины: изучение принципов сетевого взаимодействия; выработка умений настраивать и применять средства сетевого взаимодействия, использовать инструменты настройки сетевой инфраструктуры, в том числе на базе стека протоколов TCP/IP.

Дисциплина направлена на формирование следующих компетенций:

- ОПК-4.3 – Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе крипто-графических) и технических средств за-щиты информации автоматизированных систем
- ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

Знать*:*

основные положения теории информационной безопасности и практики защиты информации в телекоммуникационных сетях;

модели угроз безопасности информации;

структуру и содержание информационных процессов и особенностей функционирования объекта защиты на базе TCP/IP;

основные сервисы и механизмы шифрования и аутентификации информации по модели OSI/ISO;

модели и методы защиты сетей на базе TCP/IP;

нормативные правовые документы в области защиты информации;

требования по установке, настройке, администрированию и обслуживанию систем защиты информации в вычислительных сетях на примере МЭ, СОВ, сканеров уязвимостей.

Уметь:

осуществлять базовые настройки сетевых устройств 2-го и 3-го уровня согласно модели OSI/ISO;

обнаруживать ошибки в настройках маршрутизации;

решать типовые задачи администрирования систем защиты информации;

применять современные методы и методики защиты сетевых технологий;

организовывать мероприятия по аттестации объекта информатизации по требованиям безопасности информации; настраивать системы защиты информации в вычислительных сетях на примере МЭ, СОВ, сканеров уязвимостей.

Владеть:

навыками настройки и эксплуатации коммуникационного оборудования.

методами использования средств защиты протоколов стека TCP/IP;

навыками эксплуатации защищенных протоколов стека TCP/IP;

навыками организации и сопровождении процесса аттестации объекта информатизации по требованиям безопасности информации;

навыками по осуществлению планирования и организации работы персонала вычислительных сетей с учетом требований по защите информации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.