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) подготовки
Безопасность автоматизированных систем
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва *2021*

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
№ 10 от 20.05.2021 г.

ОГЛАВЛЕНИЕ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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**
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Способен применять соответствующий математический аппарат для решения профессиональных задач	Уметь: решать типовые криптографические задачи защиты информации;
	УК-2.2 Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения	Владеть: навыками использования положений стандартов в области безопасности вычислительных сетей при разработке, настройке и эксплуатации
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	Владеть: навыками поиска нужной информации в

	Владеет методами и средствами криптографической и технической защиты информации	нормативных базах и источниках; навыками эксплуатации криптографических протоколов и схем в вычислительных сетях

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина относится к 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», «Техническое регулирование в области защиты информации», «Информационная безопасность телекоммуникационных систем».

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

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины составляет 3 з.е., 114 часов, в том числе контактная работа обучающихся с преподавателем 60 ч., промежуточный контроль – 18 ч., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Введение в теорию и практику обеспечения безопасности сетевых технологий	7	4						Опрос

2	Базовая эталонная модель OSI/ISO. Архитектура защиты информации	7	4		4			4	Оценка выполнения практических заданий
3	Стек протоколов TCP/IP. Канальный, сетевой (межсетевой), транспортный и прикладной уровни	7	4		8			4	Оценка выполнения практических и внеаудиторных заданий
4	Реализация протоколов стека TCP/IP, протоколы Ethernet, IP, TCP, UDP. HTTP, FTP и другие	7	4		8			8	Оценка выполнения практических и внеаудиторных заданий
5	Угрозы, атаки и уязвимости в сетях на базе TCP/IP, методы и механизмы защиты от них	7	4		8			8	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых	7	4		8			4	Оценка выполнения практических заданий

	протоколов.								
7	*Экзамен*	7					18	8	Экзамен по билетам
	Итого:		**24**		**36**		**18**	**36**	

Зачет на одном из последних занятий семинарского типа.

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**	Примеры реализация протоколов стека TCP/IP, использование сетевых протоколов в современных программно-аппаратных решений.

	Ethernet, IP, TCP, UDP. HTTP, FTP и другие	
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,**	ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем.

	регламентирующие деятельность в области защиты сетевых протоколов	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* *Изучение материалов лекций*
2	*Базовая эталонная модель OSI/ISO. Архитектура защиты информации.*	*Лекция 2.1* *Лекция 2.2* *Самостоятельная работа*	*Традиционная с использованием презентаций* *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* *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* *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.*	*Традиционная с использованием презентаций* *Выполнение задания* *Изучение материалов лекций*

		Самостоятельная работа	
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* *Выполнение задания. Специализированное ПО - VPN-клиенты: ZPN-Connet, Free VPN, OpenVPN, VPN Monster, Whoer VPN, Windscribe VPN, снифффер WireShark* *Изучение материалов лекций*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос (темы 1-6)* *- участие в дискуссии на семинаре* *- практические занятия (темы 1-3)* *- практические занятия (темы 4-6)*	 *5 баллов* *5 баллов* *6 баллов* *7 баллов*	 *30 баллов* *10 баллов* *6 баллов* *24 балла*
Промежуточная аттестация *Экзамен*		*40 баллов*
Итого за семестр *Экзамен*		*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; УК-2,2, УК-2.1	Опрос

2.	Практические занятия 1 – 5	ОПК-9.1; ОПК-9.2; ОПК-9.3; УК-2,2, УК-2.1	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»/ «зачтено (отлично)»/ «зачтено»	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 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»/ «зачтено (хорошо)»/ «зачтено»	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	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	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	«неудовлетворительно»/ не зачтено	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, УК-2

Контрольные вопросы	**Реализуемые компетенции**

1. Архитектура компьютерных сетей.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
2. Модель OSI/ISO. Уровни взаимодействия в рамках компьютерных сетей. Понятие протоколов и интерфейсов.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
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, УК-2.1,УК-2.2
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, УК-2.1,УК-2.2
11. Настройка статической маршрутизации на примере оборудования Cisco.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
12. Протоколы динамической маршрутизации.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
13. Протоколы управления сетью на примере ICMP и SNMP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
14. Функции и принципы работы протоколов транспортного уровня. Заголовки протоколов TCP и UDP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
15. Системы пакетной фильтрации на примере ipfw.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
16. Назначение и принципы работы протокола DNS.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
17. Назначение и принципы работы протокола FTP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
18. Протокол HTTP, настройка HTTP-сервера на примере apache и nginx.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
19. Протоколы почтовой связи на примере POP2(IMAP) и SMTP.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2

20.Организация защищенного канала связи с использованием протокола SSL/TLS.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
21. DNS-туннелирование. Использование данной технологии для обхода межсетевых экранов.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
22. XSS-атаки на сайты.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
23. Понятие фишинга.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2
24. Утилиты nmap и hping3 для зондирования сетей.	ОПК-9.1, ОПК-9.2,ОПК-9.3, УК-2.1,УК-2.2

Примерные задания для тестирования- проверка сформированности компетенций ОПК-9, УК-2

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», необходимый для освоения дисциплины

Адреса ресурсов 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.

7. Материально-техническое обеспечение дисциплины

Для проведения занятий необходимо следующее материально-техническое обеспечение:

1. для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должны быть установлены следующее ПО:

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Microsoft Share Point 2010	Microsoft	лицензионное
4	Microsoft Office 2013	Microsoft	лицензионное
5	Windows 10 Pro	Microsoft	лицензионное
6	Kaspersky Endpoint Security	Kaspersky	Лицензионное
7	Secret Net Studio 8.4	Код безопасности	Свободное ПО, Режим доступа: https://securitycode.ru Демо-версия
8	Dallas Lock 8.0	Конфидент	Свободное ПО, Режим доступа: https://dallaslock.ru/ Демо-версия
9	Vmware Player 15.5	VMWare	Свободное ПО, Режим доступа: https://www.vmware.com/products/ Демо-версия
10	XSpider 7.0	Positive Technologies	Свободное ПО, Режим доступа: https://www.ptsecurity.com/ru-ru/ Демо-версия
11	Nmap 7.8	Nmap	Свободное ПО, Режим доступа: https://nmap.org/
12	Wireshark 3.0	Wireshark	Свободное ПО, Режим доступа: https://www.wireshark.org/
13	ZPN-Connet	ZPN	Платное ПО. Доступна trial-версия Скачать дистрибутив можно по ссылке https://zpn.im/download-free-vpn-software-windows
14	Free VPN	Free VPN	Свободное ПО.

			Настройки аккаунта для соединения с сервером доступны по адресу. https://freevpn.me/accounts/ RAR-архив с сертификаты и данными по аккаунту доступны по адресу: https://drive.google.com/file/d/1BE-7YL0eb9Xt7VM4rnPHxADBPTxjuAJx/view?usp=sharing
15	VPN Monster	Monster	Платное ПО. Доступна trial-версия Нужно зарегистрироваться на сайте и скачать ПО. https://vpnmonster.ru/files/vpnmonster.exe
16	Whoer VPN.	Whoer	Платное ПО. Доступна trial-версия. Необходимо зарегистрироваться и получить активационный код. https://whoer.net/ru/download/vpn-windows.
17	Windscribe VPN	Windscribe	Платное ПО. Доступна trial-версия Установка и настройка подключений интуитивно понятна. Скачать дистрибутив можно по ссылке https://windscribe.com/download

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

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

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, УК-2*

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

Практическое занятие 1(4 ч.). Изучение сетей Ethernet и Infiniband- ***проверка сформированности компетенций ОПК-9, УК-2)***

*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).

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.

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

Вопросы для обсуждения:

1.Перечень основных нормативно-правовых документов.

2. Понятие сеть TCP/IP.

3. Топология сетей.

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.

Практическое занятие 3(8 ч.). Модель OSI. Структура пакетов IP - *проверка сформированности компетенций ОПК-9, УК-2*

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, УК-2*

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?

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, сканер уязвимостей (XSpider), утилита nmap.

Практическое занятие 5(8 ч.). Обычный и каскадный VPN - проверка сформированности компетенций ОПК-9, УК-2

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.

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. VPN-клиенты: ZPN-Connet, Free VPN, OpenVPN, VPN Monster, Whoer VPN, Windscribe VPN, сниффер WireShark

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

«Дисциплина «Безопасность вычислительных сетей» реализуется на факультете Информационных систем и безопасности для студентов 4-го курса, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – Безопасность автоматизированных систем) 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:

- УК-2 -Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
- УК-2.1 -Способен применять соответствующий математический аппарат для решения профессиональных задач
- УК-2.2 - Способен использовать знания о важнейших нормах, институтах и отраслях действующего российского права для определения круга задач и оптимальных способов их решения
- 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
- ОПК-9.2 - Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации
- ОПК-9.3 - Владеет методами и средствами криптографической и технической защиты информации

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;

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.

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.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольной работы, тестирования, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.