

МИНОБРНАУКИ РОССИИ

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

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

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СЕТЕЙ НА БАЗЕ ТСР/П

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) подготовки
№ 3 Комплексная защита объектов информатизации
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

Безопасность информационных технологий и сетей на базе TCP/IP

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

№ 6 от 24.01.2017 г. _____

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

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

1.3. Место дисциплины в структуре образовательной программы

2. Структура дисциплины

3. Содержание дисциплины

4. Образовательные технологии

5. Оценка планируемых результатов обучения

5.1. Система оценивания

5.2. Критерии выставления оценок

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

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

7. Материально-техническое обеспечение дисциплины

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

9. Методические материалы

9.1. Планы практических занятий

Приложения

Приложение 1. Аннотация дисциплины

Приложение 2. Лист изменений

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

Коды компетенции	Содержание компетенций	Перечень планируемых результатов обучения по дисциплине
ОПК-7	должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	<p>Знать:</p> <ul style="list-style-type: none"> 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. <p>Уметь:</p> <ul style="list-style-type: none"> осуществлять базовые настройки сетевых устройств 2-го и 3-го уровня согласно модели OSI/ISO; обнаруживать ошибки в настройках маршрутизации; <p>Владеть:</p> <ul style="list-style-type: none"> навыками настройки и эксплуатации коммуникационного оборудования.
ПК-3	должен обладать способностью администрировать подсистемы информационной безопасности объекта защиты	<p>Знать:</p> <ul style="list-style-type: none"> модели и методы защиты сетей на базе TCP/IP; <p>Уметь:</p> <ul style="list-style-type: none"> решать типовые задачи администрирования систем защиты информации; применять современные методы и методики защиты сетевых технологий. <p>Владеть:</p> <ul style="list-style-type: none"> методами использования средств защиты протоколов стека TCP/IP; навыками эксплуатации защищенных протоколов стека TCP/IP.

ПК-6

должен обладать способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Знать:

нормативные правовые документы в области защиты информации;

Уметь:

организовывать мероприятия по аттестации объекта информатизации по требованиям безопасности информации.

Владеть:

навыками организации и сопровождения процесса аттестации объекта информатизации по требованиям безопасности информации.

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина относится к вариативной части частью блока дисциплин учебного плана.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: "Математические основы защиты информации", "Вычислительные сети", «Сети и системы передачи данных», «Информационные технологии», «Техническое регулирование в области защиты информации».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практик: «Организация виртуальных частных сетей», «Проектирование систем защиты объектов информатизации», «Преддипломная практика».

2. Структура дисциплины

Структура дисциплины для очной формы обучения

Общая трудоемкость дисциплины – 3 з.е., 108 часов, в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 66 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	2						Опрос
2	Базовая эталонная модель OSI/ISO. Архитектура защиты информации	7	4					4	Оценка выполнения практических заданий
3	Стек протоколов TCP/IP. Канальный, сетевой (межсетевой), транспортный и прикладной уровни	7	4		8			8	Оценка выполнения практических и внеаудиторных заданий
4	Реализация протоколов стека	7	4		6			8	Оценка выпол-

	TCP/IP, протоколы Ethernet, IP, TCP, UDP. HTTP, FTP и другие								нения практических и внеаудиторных заданий
5	Угрозы, атаки и уязвимости в сетях на базе TCP/IP, методы и механизмы защиты от них	7	4		4			16	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых протоколов.	7	4		2			20	Оценка выполнения практических заданий
7	<i>Зачет</i>	7						10	Зачет по билетам
	Итого:		22		20			66	

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 понятия. 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	<p>Стек протоколов TCP/IP. Поля и флаги пакетов. Применение 4 уровней при разработке средств защиты информации.</p> <p>Особенности семейства протоколов TCP/IP и сетей на его основе. Стек протоколов TCP/IP включает в себя:</p> <ul style="list-style-type: none"> • 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,

		<p>подтверждение в получении сообщения;</p> <ul style="list-style-type: none"> • 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	<p>Примеры реализации протоколов стека TCP/IP, использование сетевых протоколов в современных программно-аппаратных решениях.</p>
5	Угрозы, атаки и уязвимости в сетях на базе TCP/IP, методы и механизмы защиты от них	<p>Современные угрозы в сетях на базе TCP/IP.</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>Следующая группа методов защиты от удалённых атак – программно-аппаратные. К ним относятся:</p> <ul style="list-style-type: none"> • 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. Самостоятельная работа	Традиционная с использованием презентаций Изучение материалов лекций
2	Базовая эталонная модель OSI/ISO. Архитектура защиты информации.	Лекция 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 1. 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 Практическое занятие 2. 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 Практические занятие 3. Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых протоколов	Лекция 6.1 Самостоятельная работа	Традиционная с использованием презентаций Выполнение задания Изучение материалов лекций

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос	5 баллов	30 баллов
- участие в дискуссии на семинаре	5 баллов	10 баллов
- контрольная работа (темы 1-2)	10 баллов	10 баллов
- контрольная работа (темы 3-6)	10 баллов	10 баллов
Промежуточная аттестация		40 баллов
Зачет		
Итого за семестр		100 баллов
Зачет		

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»	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>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.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	<p>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.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	<p>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.</p> <p>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.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	«неудовлетворительно»/ не зачтено	<p>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.</p> <p>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.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

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

Контрольные вопросы к зачету - проверка сформированности компетенций ОПК-7, ПК-3, ПК-6

1. Архитектура компьютерных сетей.
2. Модель OSI/ISO. Уровни взаимодействия в рамках компьютерных сетей. Понятие протоколов и интерфейсов.
3. Стек протоколов TCP/IP. Процедура инкапсуляции.
4. Физический и канальные уровни модели OSI/ISO. Топология сетей. Коммуникационное оборудование канального уровня.
5. Формат кадра Ethernet. Технология CSMA/CD.
6. Принципы построения сетей, сегментированных на канальном уровне.
7. Назначение и принципы работы протоколов ARP/RARP. Атака ARP-spoofing.
8. Функции и принципы реализации протокола IP. Формат заголовка IP.
9. Фрагментирование IP пакетов. MTU.
10. Настройка сетевого интерфейса в ОС Microsoft и Unix. Статическая маршрутизация.
11. Настройка статической маршрутизации на примере оборудования Cisco.
12. Протоколы динамической маршрутизации.
13. Протоколы управления сетью на примере ICMP и SNMP.
14. Функции и принципы работы протоколов транспортного уровня. Заголовки протоколов TCP и UDP.
15. Системы пакетной фильтрации на примере ipfw.
16. Назначение и принципы работы протокола DNS.
17. Назначение и принципы работы протокола FTP.
18. Протокол HTTP, настройка HTTP-сервера на примере apache и nginx.
19. Протоколы почтовой связи на примере POP2(IMAP) и SMTP.
20. Организация защищенного канала связи с использованием протокола SSL/TLS.
21. DNS-туннелирование. Использование данной технологии для обхода межсетевых экранов.
22. XSS-атаки на сайты.
23. Понятие фишинга.
24. Утилиты nmap и hping3 для зондирования сетей.

Примерные задания для тестирования- проверка сформированности компетенций ОПК-7, ПК-3, ПК-6

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-спуфинг – это:

- а) стек сетевого устройства.
- б) подделывание MAC-адреса сетевого устройства.
- в) HTTP запрос.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

1. *Руководящий документ*. 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-gostekhkommisii-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-gostekhkommisii-rossii-ot-30-marta-1992-g>, свободный. – Загл. с экрана.

Основная литература

1. *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>
2. *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, кор. 1997-2018. – Режим доступа: www.consultant.ru.

7. Материально-техническое обеспечение дисциплины

1) лекционный класс с видеопроектором и компьютером, на котором должны быть установлены:

- лицензионное ПО MS Windows 7 и старше;
- лицензионное ПО MS Office 2010 (с обязательным наличием MS PowerPoint) и старше

2) компьютерный класс, оборудованный современными персональными компьютерами для каждого студента с выходом в интернет. На компьютере должны быть установлены:

- лицензионное ПО MS Windows 7 и старше;
- лицензионное ПО MS Office 2010 и старше;
- программный гипервизор VMware Player;
- сканер уязвимостей (XSpider);
- утилита nmap, сниффер Wireshark.

Перечень 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/

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

Перечень БД и ИСС

№п /п	Наименование
1	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, регулируемые эргономическими партами СИ-1;

– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - проверка сформированности компетенций ОПК-7, ПК-3, ПК-6

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(8 ч.). Нормативно-методическая база использования. Краткий обзор руководящих документов (проверка сформированности компетенций ОПК-7, ПК-3)

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 2(6 ч.). Модель OSI. Структура пакетов IP (проверка сформированности компетенций ПК-3, ПК-6)

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 3(4 ч.). Угрозы, атаки и уязвимости в сетях на базе TCP/IP (проверка сформированности компетенций ОПК-7, ПК-3, ПК-6)

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.

АННОТАЦИЯ ДИСЦИПЛИНЫ

Дисциплина «Безопасность информационных технологий и сетей на базе TCP/IP» реализуется на факультете Информационных систем и безопасности для студентов, обучающихся по программе бакалавриата по направлению подготовки 10.03.01 Информационная безопасность (профили подготовки – № 3 Комплексная защита объектов информатизации) 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-7 – должен обладать способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.
- ПК-3 – должен обладать способностью администрировать подсистемы информационной безопасности объекта защиты.
- ПК-6 – должен обладать способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств 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, реферата, тестирования, промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	<i>29.06.2017г.</i>	10
2	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	<i>26.06.2018 г.</i>	11
3	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2019 г.)</i>	<i>29.08.2019 г</i>	1
4	<i>Обновлена основная и дополнительная литература</i>	<i>29.08.2019 г</i>	1
5	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	<i>29.08.2019 г</i>	1
6	<i>Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)</i>	<i>23.06.2020</i>	14
7	<i>Обновлена основная и дополнительная литература</i>	<i>23.06.2020</i>	14
8	<i>Обновлен раздел п.4 Образовательные технологии</i>	<i>23.06.2020</i>	14
9	<i>Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)</i>	<i>23.06.2020</i>	14

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)
Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель: К.т.н, доцент, А.С. Моляков

2. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) (2018 г.)**Перечень ПО**

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

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

3. Обновление структуры дисциплины (модуля) для очной формы обучения (2019 г.)**Структура дисциплины (модуля) для очной формы обучения**

Общая трудоемкость дисциплины – 3 з.е., 108 часов, в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 66 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	2						10	Опрос
2	Базовая эталонная модель OSI/ISO. Архитектура защиты информации	7	4						4	Оценка выполнения практических заданий
3	Стек протоколов TCP/IP. Канальный, сетевой (межсетевой), транспортный и прикладной уровни	7	4		8				8	Оценка выполнения практических и внеаудиторных заданий
4	Реализация протоколов стека TCP/IP, протоколы Ethernet, IP, TCP, UDP. HTTP, FTP и другие	7	4		6				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		4				16	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых протоколов.	7	4		2				20	Оценка выполнения практических заданий
7	Зачет с оценкой	7								Зачет с оценкой по билетам
	Итого:		22		20				66	

4. Обновление основной и дополнительной литературы (2019 г.)

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

Дополнить раздел Основная литература

Гаврилов, М. В. Информатика и информационные технологии : учебник для прикладного бакалавриата / М. В. Гаврилов, В. А. Климов. – 4-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2019. – 383 с. – (Серия : Бакалавр. Прикладной курс). – ISBN 978-5-534-00814-2. – Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/bcode/431772>

Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/1025261> (дата обращения: 11.08.2019)

Дополнить раздел Дополнительная литература

Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Серия : Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715>.

5.Обновление состава программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

Перечень ПО

№ п/п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№ п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной

	подписки в 2019 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 Grebennikov.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:

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

6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)**Структура дисциплины для очной формы обучения**

Общая трудоемкость дисциплины – 3 з.е., 114 часов, в том числе контактная работа обучающихся с преподавателем 42 ч., самостоятельная работа обучающихся 72 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	2					10	Опрос
2	Базовая эталонная модель OSI/ISO. Архитектура защиты информации	7	4					4	Оценка выполнения практических заданий
3	Стек протоколов TCP/IP. Канальный, сетевой (межсетевой), транспортный и прикладной уровни	7	4		8			8	Оценка выполнения практических и внеаудиторных заданий
4	Реализация протоколов стека TCP/IP, протоколы Ethernet, IP, TCP, UDP. HTTP, FTP и другие	7	4		6			10	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		4			18	Оценка выполнения практических и внеаудиторных заданий
6	Отечественные нормативные акты, регламентирующие деятельность в области защиты сетевых протоколов.	7	4		2			22	Оценка выполнения практических заданий
7	Зачет с оценкой	7							Зачет с оценкой по билетам
	Итого:		22		20			72	

7. Обновление основной и дополнительной литературы (2020 г.)

В раздел 6. Учебно-методическое и информационное обеспечение дисциплины вносятся следующие изменения:

Дополнить раздел Основная литература

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>

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>

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>

Дополнить раздел **Дополнительная литература**

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>

8. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ. для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

9. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

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
--	-----------------------------

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Состав программного обеспечения (ПО)

№ п/п	Наименование ПО	Производитель	Способ распространения (<i>лицензионное или свободно распространяемое</i>)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

К.т.н, доцент, А.С. Моляков