Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.О.37
Безопасность компьютерных сетей
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 48
самостоятельная работа 59,8
контактная работа во время промежуточной аттестации (ИКР) 0

Виды контроля в семестрах:
зачеты 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	16 1/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	32	32	32	32
Контактная работа на аттестации	0,2	0,2	0,2	0,2
В том числе в форме практ.подготовки	8	8	8	8
Итого ауд.	48	48	48	48
Контактная работа	48,2	48,2	48,2	48,2
Сам. работа	59,8	59,8	59,8	59,8
Итого	108	108	108	108

Программу составил(и):
к.т.н., доцент, Капустин С.А.

Рецензент(ы):
д.т.н., Профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Безопасность компьютерных сетей

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Понимание угроз и рисков безопасности компьютерных сетей
1.2	Изучение архитектуры компьютерных сетей
1.3	Разработка и внедрение политик безопасности
1.4	Изучение методов обнаружения и анализа инцидентов безопасности
1.5	Разработка стратегий безопасности
1.6	Понимание юридических и этических аспектов безопасности

Задачи: 1. Изучение основных принципов безопасности компьютерных сетей
2. Ознакомление с методами аутентификации и авторизации
3. Разработка политик безопасности
4. Изучение методов обнаружения и предотвращения атак
5. Изучение сетевой безопасности и защиты данных
6. Анализ и реагирование на инциденты безопасности
7. Обучение мерам безопасности для сетевых приложений
8. Ознакомление с соответствующими правовыми и этическими аспектами безопасности компьютерных сетей

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Гуманитарные аспекты информационной безопасности
2.1.2	Интеллектуальные системы и технологии
2.1.3	Сети и телекоммуникации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Специализированные вычислительные устройства защиты информации
2.2.2	Комплексная защита объектов информатизации
2.2.3	Порядок проведения аттестации объектов информатизации

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	
ОПК-9.1: Использует средства криптографической защиты информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний средств криптографической защиты информации в автоматизированных системах
Уровень 2	Уровень знаний средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний средств криптографической защиты информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок
ОПК-9.2: Решает задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов	
Уметь	
Уровень 1	Продемонстрированы основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения решать задачи криптографической защиты информации с использованием блочных и поточных систем шифрования, криптографических систем с открытым ключом, криптографических хеш-функций и криптографических протоколов, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.3: Организует защиту информации от утечки по техническим каналам на объектах информатизации	
Владеть	
Уровень 1	Имеется минимальный набор навыков для организации защиты информации от утечки по техническим каналам на объектах информатизации с негрубыми ошибками и некоторыми недочётами

Уровень 2	Продемонстрированы базовые навыки для организации защиты информации от утечки по техническим каналам на объектах информатизации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки для организации защиты информации от утечки по техническим каналам на объектах информатизации без ошибок и недочётов
ОПК-9.4: Оценивает угрозы информационной безопасности объекта информатизации	
Уметь	
Уровень 1	Продемонстрированы основные умения оценивать угрозы информационной безопасности объекта информатизации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения оценивать угрозы информационной безопасности объекта информатизации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения оценивать угрозы информационной безопасности объекта информатизации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-9.5: Использует средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки использования средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки использования средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации без ошибок и недочётов

ОПК-10: Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	
ОПК-10.1: Реализует требования политик безопасности на объектах информатизации	
Знать	
Уровень 1	Знает требования политик безопасности на объектах информатизации, но реализует с ошибками
Уровень 2	Знает требования политик безопасности на объектах информатизации, но реализует с незначительными ошибками
Уровень 3	Знает требования политик безопасности на объектах информатизации, реализует без ошибок
ОПК-10.2: Конфигурирует программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности	
Уметь	
Уровень 1	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, но допускает
Уровень 2	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности, но допускает незначительные ошибки
Уровень 3	Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности без ошибок
ОПК-10.3: Применяет средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях	
Владеть	
Уровень 1	Выполняет настройку средств защиты информации с ошибками
Уровень 2	Выполняет настройку средств защиты информации с незначительными ошибками
Уровень 3	Выполняет настройку средств защиты информации без ошибок

ОПК-4.4: Способен осуществлять диагностику и мониторинг систем защиты автоматизированных систем;	
ОПК-4.4.1: Применяет инструментальные средства контроля защищенности информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний инструментальных средств контроля защищенности информации в автоматизированных системах
Уровень 2	Уровень знаний инструментальных средств контроля защищенности информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний инструментальных средств контроля защищенности информации в автоматизированных

	системах в объёме, соответствующем программе подготовки, без ошибок
ОПК-4.4.2: Документирует действия по устранению неисправностей в работе системы защиты информации автоматизированной системы	
Уметь	
Уровень 1	Продемонстрированы основные умения документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения документировать действия по устранению неисправностей в работе системы защиты информации автоматизированной системы, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ОПК-4.4.3: Регистрирует события, связанные с защитой информации в автоматизированных системах	
Владеть	
Уровень 1	Имеется минимальный набор навыков регистрировать события, связанные с защитой информации в автоматизированных системах с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки регистрировать события, связанные с защитой информации в автоматизированных системах с некоторыми недочётами
Уровень 3	Продемонстрированы навыки регистрировать события, связанные с защитой информации в автоматизированных системах без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература и эл. ресурсы	Практ. подг.
	Раздел 1. Раздел 1					
1.1	Основные понятия системы передачи данных. Концепция сети /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.2	Основные понятия системы передачи данных. Концепция сети /Ср/	6	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.3	Основные понятия системы передачи данных. Концепция сети /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1

1.4	Локальные вычислительные сети, расширение компьютерных сетей. Назначение компьютерной сети. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.5	Локальные вычислительные сети, расширение компьютерных сетей. Назначение компьютерной сети. /Ср/	6	8,2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.6	Локальные вычислительные сети, расширение компьютерных сетей. Назначение компьютерной сети. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
1.7	Одноранговые сети, размеры сети, стоимость сети, операционные системы, реализация, целесообразность применения. Сети на основе сервера, специализированные серверы, значение программного обеспечения /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.8	Одноранговые сети, размеры сети, стоимость сети, операционные системы, реализация, целесообразность применения. Сети на основе сервера, специализированные серверы, значение программного обеспечения /Ср/	6	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.9	Одноранговые сети, размеры сети, стоимость сети, операционные системы, реализация, целесообразность применения. Сети на основе сервера, специализированные серверы, значение программного обеспечения /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1

1.10	Функционирование сети. Работа сети, модель OSI, многоуровневая архитектура. Взаимодействие уровней модели OSI. Модель IEEE Project 802, расширение модели OSI. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.11	Функционирование сети. Работа сети, модель OSI, многоуровневая архитектура. Взаимодействие уровней модели OSI. Модель IEEE Project 802, расширение модели OSI. /Ср/	6	8,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.12	Функционирование сети. Работа сети, модель OSI, многоуровневая архитектура. Взаимодействие уровней модели OSI. Модель IEEE Project 802, расширение модели OSI. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
1.13	Назначение драйверов. Сетевая среда, драйверы и модель OSI. Драйверы и сетевое программное обеспечение, драйвер платы сетевого адаптера. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.14	Назначение драйверов. Сетевая среда, драйверы и модель OSI. Драйверы и сетевое программное обеспечение, драйвер платы сетевого адаптера. /Ср/	6	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.15	Назначение драйверов. Сетевая среда, драйверы и модель OSI. Драйверы и сетевое программное обеспечение, драйвер платы сетевого адаптера. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1

1.16	Функции пакетов данных. Структура пакета, основные компоненты. Формирование пакетов, адресация пакета, рассылка пакетов. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.17	Функции пакетов данных. Структура пакета, основные компоненты. Формирование пакетов, адресация пакета, рассылка пакетов. /Ср/	6	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.18	Функции пакетов данных. Структура пакета, основные компоненты. Формирование пакетов, адресация пакета, рассылка пакетов. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
1.19	Маршрутизируемые и немаршрутизируемые протоколы. Стандартные стеки. Стандартные протоколы /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.20	Маршрутизируемые и немаршрутизируемые протоколы. Стандартные стеки. Стандартные протоколы /Ср/	6	6,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.21	Маршрутизируемые и немаршрутизируемые протоколы. Стандартные стеки. Стандартные протоколы /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1

1.22	Понятие о коммутируемой транспортной сети. Методы коммутации, их достоинства и недостатки. Коммутация цепей (линий). Коммутация сообщений. Коммутация пакетов. Принципы пакетной передачи данных. Коммутация символов. /Лек/	6	2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.23	Понятие о коммутируемой транспортной сети. Методы коммутации, их достоинства и недостатки. Коммутация цепей (линий). Коммутация сообщений. Коммутация пакетов. Принципы пакетной передачи данных. Коммутация символов. /Ср/	6	8,8	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	
1.24	Понятие о коммутируемой транспортной сети. Методы коммутации, их достоинства и недостатки. Коммутация цепей (линий). Коммутация сообщений. Коммутация пакетов. Принципы пакетной передачи данных. Коммутация символов. /Лаб/	6	4	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	1
	Раздел 2. Промежуточная аттестация					
2.1	Зачет /КА/	6	0,2	ОПК-9.1 ОПК-9.2 ОПК-9.3 ОПК-9.4 ОПК-9.5 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-4.4.1 ОПК-4.4.2 ОПК-4.4.3	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Классификация сетевых угроз
2. Сетевые атаки, реализуемые на физическом уровне модели OSI
3. Атаки на коммутаторы. Переполнение CAM-таблицы, атаки на STP, MAC, ARP – спуффинг
4. Безопасность протоколов статической маршрутизации. Обеспечение безопасности протокола RIP.
5. Атаки на протоколы динамической маршрутизации. Безопасность протокола OSPF.
6. Атаки на TCP. IP-spoofing.
7. Классификация сетевых средств защиты информации
8. Нормативные документы ФСТЭК и ФСБ России, регулирующие процесс обеспечения сетевой безопасности в государственных инфор-мационных системах.
9. Виды и классификация VPN
10. Возможности комплекса криптографической защиты VipNet.
11. Порядок создания защищенной VPN-сети VipNet
12. Механизмы разграничение доступа к ресурсам в сети VipNet
13. Аппаратные решения комплекса VipNet
14. Типовые схемы использования комплекса VipNet в локальной вычислительной сети
15. Дополнительные возможности комплекса VipNet (помимо построения VPN сети)
16. Сетевые сканеры

17. Системы IDS и IPS

5.2. Темы письменных работ

1. Создание удостоверяющего центра на базе ПАК «Крипто Про УЦ»
2. Разработка сетевого анализатора с использованием библиотека scapy
3. Использование Microsoft System Center для мониторинга информационной инфраструктуры и реагирования на инциденты
безопасности
4. Безопасная настройка беспроводной точки доступа для подключения к корпоративным информационным ресурсам
5. Применение криптопровайдера VipNet CSP в стандартных приложениях
6. Настройка прокси-сервера SQUID в типовой локальной вычислительной сети
7. Использование системы Zabbix для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности
8. Сравнение программных межсетевых экранов: VipNet Firewall, SSEP, Kaspersky
9. Настройка политик безопасности в сетевой версии SecretNet для обеспечения безопасности типовой государственной информационной системы.
10. Защита корпоративной информации от утечек с использованием программного решения Secure Tower
11. Настройка ОС AstraLinux по требованиям безопасности информации
12. Использование библиотеки winpcap для создании системы сетевой безопасности
13. Использование системы snort для обеспечения безопасности ЛВС
14. Использование ОС Kali Linux для анализа защищенности сетевых ресурсов

5.3. Фонд оценочных средств

1. Метод защиты от атаки переполнение CAM-таблицы
А) Включение Port-security на всех access-портах
Б)Принудительный выбор Root-порта
В) Отключение CAM-таблицы
Г)Использование маршрутизатора вместо коммутатора
2. Одной из разновидностей атак на протокол STP является
А) «вечный цикл»
Б)«вечная маршрутизация»
В) «вечные выборы»
Г) «вечная коммутация»
3. Какой из представленных программных продуктов не обеспечивает перехват и анализ трафика?
А) Wireshark
Б) Terrier
В) Tcpdump
Г) SmartSniff
4. Атака Arp-Spoofing относится к следующему типу атак:
А) Brute-force
Б) DOS
В) ZeroDay
Г) MITM
5. Одним из возможных последствий успешной реализации атаки «переполнение MAC-таблицы» может являться следующее:
А) концентратор начинает работать в режиме коммутатора
Б) коммутатор начинает работать в режиме концентратора
В) маршрутизатор начинает работать в режиме коммутатора
Г) маршрутизатор начинает работать в режиме концентратора
6. Port-security – это функция...
А) маршрутизатора, позволяющая отфильтрофать трафик на каждом порту, не удовлетворяющий заданным критериям
Б) коммутатора, позволяющая отфильтровать траффик в соответствие с таблицей маршрутизации
В) коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт
Г) маршрутизатора, позволяющая указать безопасные ip-адреса хостов, от которых разрешена маршрутизация трафика
7. Выберите верное завершение предложения: «все коммутаторы, подключенные к пораженному атакой «переполнение CAM-таблицы» ….»
А) очистят все записи в своих CAM-таблицах
Б)также подхватят фальшивые MAC-адреса и начнут вести широковещательную рассылку всех кадров
В)моментально потеряют с ним связь до того момента, пока атака не будет нейтрализована
Г) очистят все записи в своих ARP-таблицах
8. Какой из перечисленных терминов не является режимом реагирования функции коммутатора port security
А)protect
Б)restrict
В)shutdown
Г)update
9. Какое слово пропущено DHCP-##### — это функция коммутатора, предназначенная для защиты от атак с использованием
протокола DHCP. Например, атаки с подменой DHCP-сервера в сети или атаки DHCP starvation
А)scanning

Б)spoofing
В)snooping
Г)streaming
УП: v10.03.01_2023_Информационная безопасность.plx стр. 10
10. MAC-spoofing –это атака ###### уровня модели OSI
А)канального
Б)транспортного
В)прикладного
Г)сетевого

1. Выберите верное высказывание
А) К пакету применяются все перечисленные в списке доступа условия
Б) Условия применяются
к пакету в том порядке, в котором они перечисляются в списке доступа до первого совпадения (оставшиеся условия не проверяются)
В) К пакету применяется только первое условие, содержащееся в списке доступа
Г) Условия применяются к пакету в том порядке, в котором они были добавлены администратором при его редактировании
2. Syslog сообщение – это ….
А) информация в закодированном виде об, facility и Severity level, HEADER, TIMESTAMP, имени или IP адресе хоста в десятичной записи (HOSTNAME), а так же (MSG).
Б) стандарт отправки сообщений о происходящих в системе событиях (логов), использующийся в компьютерных сетях, работающих по протоколу IP.
В) Протокол передачи текстовых сообщений, прежде всего логов — сообщений о происходящих событиях.
Г) сообщение операционной системы об обнаружении атаки типа MITM
3. Выберите верное выражение
А) Протокол Telnet – ключевой протокол для удалённого администрирования различными сетевыми устройствами и программными серверами
Б) Протокол Telnet больше не поддерживается современными сетевыми устройствами
В) Протокол Telnet – проприетарный протокол для удаленного администрирования оборудования компании Cisco
Г) Протокол Telnet использовался для удалённого администрирования различными сетевыми устройствами и программными
серверами, но уступил протоколу SSH из-за безопасности
4. Как называется метод атаки с угадыванием паролей, учетных данных для входа в систему, ключей шифрования и прочей информации.
А)MITM
Б) DOS
В) DDOS
Г)Bruteforce
5. Структурированное представление всей информации, влияющей на безопасность конкретной информационной системы (ИС), которое включает в себя расчет рисков воплощения угрозы в жизнь, а также оценку предполагаемых последствий называется
А) Технический паспорт ИС
Б) Сетевая политика безопасности
В)Модель угроз
Г)Банк данных угроз

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Кузин А. В., Кузин Д.А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2020, URL: http://znanium.com/catalog/document?id=357755
Л1.2	Максимов Н. В., Попов И.И.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2023, URL: https://znanium.com/catalog/document?id=428554
Л1.3	Кузин А. В., Кузин Д.А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2023, URL: https://znanium.com/catalog/document?id=429500

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Артюшенко В.В., Никулин А.В.	Компьютерные сети и телекоммуникации: Учебно-методическая литература	Новосибирск: Новосибирский государственный технический университет (НГТУ), 2020, URL: https://znanium.com/catalog/document?id=396946
Л2.2	Максимов Н. В., Попов И.И.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2020, URL: https://znanium.com/catalog/document?id=352328

6.2. Электронные учебные издания и электронные образовательные ресурсы	
Э1	Интернет университет информационных технологий ИНТУИТ . - Режим доступа: https://www.intuit.ru/studies/courses
Э2	Федеральный центр информационно-образовательных ресурсов . - Режим доступа: http://fcior.edu.ru/
Э3	Естественно-научный образовательный портал. - Режим доступа: http://www.en.edu.ru/
Э4	Единое окно доступа к образовательным ресурсам . - Режим доступа: http://window.edu.ru
Э5	Электронная библиотечная система Znanium. - Режим доступа: http://new.znanium.com/
Э6	Электронная библиотечная система Ibooks . - Режим доступа: http://www.ibooks.ru
Э7	Электронная библиотечная система BOOK.ru . - Режим доступа: http://www.book.ru
Э8	Электронные ресурсы Академии ИМСИТ . - Режим доступа: http://eios.imsit.ru/
Э9	Web-ресурс «Официальный сайт Академии ИМСИТ . - Режим доступа: http://imsit.ru
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	
6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Кодекс – Профессиональные справочные системы https://kodeks.ru
6.3.2.2	Консультант Плюс http://www.consultant.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
114а	Лаборатория сетей и систем передачи информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-

		PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational Micro-Cap Evaluation vGate Secren Net Studio Astra Linux Special Edition	USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
121	Компьютерный класс	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++.	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

		Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Безопасность компьютерных сетей». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.
Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Безопасность компьютерных сетей».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и

инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями