МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе
_____ Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность сетей ЭВМ
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Безопасность сетей ЭВМ» является формирование у студентов теоретических знаний в области безопасности сетей ЭВМ, а также навыков практического применения полученных знаний.

Задачи изучения дисциплины: изучение таких разделов, как основы безопасности сетей ЭВМ, управления доступом, методы доступа к каналам связи сети, технологии построения локальных сетей ЭВМ, безопасность на различных уровнях сетей ЭВМ, безопасность беспроводных сетей.

Дисциплина направлена на формирование общепрофессиональных (ОПК-12) компетенций выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть БЛОКА 1 «Дисциплины (модули)» подготовки студентов по специальности 10.05.03 Информационная безопасность автоматизированных систем (10.05.03-05 Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности.

Основывается на базе дисциплин: ««Информатика», «Электроника и схемотехника ЭВМ», «Дискретная математика», «Теория информации», «Сети и системы передачи информации».

Является основой для изучения следующих дисциплин: «Защита информации от утечки по техническим каналам», «Администрирование информационных систем и служб».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с применением вычислительных систем.

Курс является фундаментом для ориентации студентов в сфере разработки информационных систем.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 ак.ч. Программой дисциплины предусмотрены лекционные (36 ак.ч.), лабораторные (36 ак.ч.) занятия, самостоятельная работа студента (36 ак.ч.).

Дисциплина изучается на 4 курсе в 7 семестре. Форма промежуточной аттестации – экзамен.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Безопасность сетей ЭВМ» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 – Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12	ОПК-12.1 Применяет знания в области безопасности вычислительных сетей при разработке автоматизированных систем

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 3 зачётных единицы, 108 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		7
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	-	-
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	36	36
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	9	9
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	-	-
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	–	–
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	–	–
Работа в библиотеке	–	–
Подготовка к экзамену	18	18
Промежуточная аттестация – экзамен (Э)	Э	Э
Общая трудоемкость дисциплины		
ак.ч.	108	108
з.е.	3	3

5 Содержание дисциплины

С целью освоения компетенций, приведенных в п.3 дисциплина разбита на 3 темы:

– тема 1 (Общие сведения о безопасности сетей ЭВМ);

– тема 2 (Принципы построения сетей ЭВМ);

– тема 3 (Безопасность сетей ЭВМ).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Общие сведения о безопасности сетей ЭВМ	Общие сведения о безопасности сетей ЭВМ	2	–	–	Сетевая настройка рабочей станции	4
2	Принципы построения сетей ЭВМ	Физический и канальный уровень построения сетей ЭВМ Технологии построения локальных сетей ЭВМ Сетевой уровень построения сетей ЭВМ	4 4 4	–	–	Аудит безопасности протокола SNMP. Виртуальные локальные сети и IEEE 802.1. Протокол SSH.	4 4 4
3	Безопасность сетей ЭВМ	Безопасность транспортной подсистемы сетей ЭВМ Безопасность уровня приложений. Программно-технические средства защиты сетей ЭВМ Безопасность беспроводных сетей	6 6 6 4	–	–	Базовые механизмы безопасности коммутаторов. Списки контроля доступа ACL. Знакомство с брандмауэром Безопасность сетей WiFi.	6 6 4 4
Всего аудиторных часов		36		-		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-12	Экзамен	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– лабораторные работы – всего 100 баллов.

Оценка по экзамену проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Экзамен по дисциплине «Безопасность сетей ЭВМ» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку в форме устного собеседования по приведенным ниже вопросам.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 – Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашнее задание не предусмотрено.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Рефераты (индивидуальные задания) не предусмотрены.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1. Общие сведения о безопасности сетей ЭВМ.

1. Информационная безопасность зависит от:

а) компьютеров, поддерживающей инфраструктуры

б) пользователей

в) информации

2. Таргетированная атака – это:

а) атака на сетевое оборудование

б) атака на компьютерную систему крупного предприятия

в) атака на конкретный компьютер пользователя

3. Укажите устройство для подключения компьютера к сети:

а) мышь

б) модем

в) сканер

4. Что НЕ поможет защитить свою электронную почту от взлома:

а) периодически менять адрес электронной почты, менять провайдеров

б) создавать разные пароли от разных аккаунтов

в) не открывать сообщения с незнакомых и подозрительных адресов

5. Какие вирусы активизируются в самом начале работы с операционной системой:

а) загрузочные вирусы

б) троянцы

в) черви

Тема 2. Принципы построения сетей ЭВМ.

1. Какое действие не выполняет DSU?

а) выполняет синхронизацию

б) осуществляет выравнивание загрузки канала

в) осуществляет усиление или ослабление сигнала

г) формирует кадры каналов

2. Какой существует специальный термин для Internet, применяющийся в тех случаях, когда технология Internet переносится на корпоративную сеть?

а) Ethernet

б) Fast Ethernet

в) Intranet

г) Arc Net

3. Какое ограничение позволяет преодолеть технология виртуальных локальных сетей?

а) барьеры на пути широковещательного трафика;

б) ограничение размера пакета;

в) ограничение скорости передачи данных;

г) количество соединенных станций.

4. Какая сеть использует режим коммутации каналов?

а) Frame Relay;

б) ISDN;

в) X.25;

г) ATM.

5. Какой уровень семиуровневой архитектуры устанавливает стандартные способы представления данных, которые требуют прикладные процессы пользователей?

а) представительный

б) прикладной;

в) сеансовый;

г) физический.

Тема 3. Безопасность сетей ЭВМ.

1. Сетевой адаптер, работающий в селективном режиме, игнорирует …

а) только фреймы, не содержащие в поле «Адрес получателя» адрес данного узла

б) фреймы, не содержащие в поле «Адрес получателя» адрес данного узла, а также широковещательные фреймы

в) исключительно широковещательные фреймы

2. Адрес … используется для отправки широковещательных сообщений в данный сетевой сегмент

а) 255.255.255.255

б) 192.32.64.255

в) 255.255.255.

г) 0 0.0.0.0

3. Набор данных, который позволяет поставить открытый ключ с объектом, имеющим соответствующий закрытый ключ, носит название …

а) конструктивный сертификат

б) модуль доступа

в) цифровой сертификат

4. Управление доступом – это ...

а) защита персонала и ресурсов

б) реагирование на попытки несанкционированного доступа

в) способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных)

5. Угроза системе передачи данных – это ...

а) раскрытие информации и прерывание обслуживания

б) хищение, удаление или потеря информации и/или других ресурсов

в) опасность искажения или модификации информации

г) опасность, состоящая в разрушении информации или других ресурсов

6.5 Вопросы для подготовки к экзамену

1) Какие Вы знаете виды компьютерных сетей и их назначение?

2) Какие Вы знаете последствия и угрозы информационное безопасности?

3) Какие Вы знаете объекты информационной безопасности?

4) Что такое многоаспектная классификация ЛВС и классификационные группы?

5) В чем особенности построения, достоинства и недостатки одноранговых ЛВС и серверных ЛВС?

6) Что такое классификация компьютерных сетей по типу?

7) Что такое сетевая модель OSI?

8) Какие Вы знаете задачи и функции по уровням модели?

9) Что такое стек протоколов? Основные стеки?

10) Какие Вы знаете соответствия протоколов модели OSI?

11) Какие Вы знаете методы доступа к каналам связи сети и их отличительные особенности?

12) Что такое характеристика сетевой технологии IEEE 802?1/Ethernet и её разновидностей?

13) Что такое характеристика сетевой технологии IEEE 802?1/TokenRing?

14) Что такое краткая характеристика сетевой технологии ARCNET?

15) Что такое краткая характеристика сетевой технологии FDDI?

16) Что такое топология сети?

17) Что такое топологии типа «звезда», «кольцо», «шина»?

18) Что такое сетевая модель OSI? Физический уровень: функции, протоколы?

19) Что такое сетевая модель OSI? Канальный уровень: функции, протоколы?

20) Какие Вы знаете протоколы разрешения адресов ARP, RARP?

21) В чем назначение протокола STP и его разновидностей?

22) Что такое устройства межсетевого интерфейса?

23) Какие Вы знаете основные рейтинговые параметры ЛВС?

24) Какие Вы знаете основные принципы работы и протоколы Интернет?

25) Какие Вы знаете общие проблемы информационной безопасности?

26) Что такое VLAN, тегированный трафик?

27) Что такое протокол 802?1q?

28) Что такое аспект безопасности при сегментации трафика?

29) Основные протоколы, используемые в Интернет на сетевом уровне? В чем проблемы использования этих протоколов?

30) Какие Вы знаете системы адресации, используемые в сети Интернет?

31) Что такое сетевая модель OSI? Сетевой уровень: функции, протоколы?

32) Что такое стек протоколов TCP/IP? Алгоритмы маршрутизации, их характеристика?

33) Что такое спуфинг и снифинг? Механизмы их реализаций?

34) Что такое WinPCap, WinDivert, Wireshark?

35) Какие Вы знаете основные протоколы, используемые в Интернет на транспортном уровне? Проблемы использования этих протоколов?

36) Что такое сетевая модель OSI? Транспортный уровень: функции, протоколы?

37) Что такое туннелирование, виртуальные частные сети?

38) Какие Вы знаете ассиметричные и симметричные алгоритмы шифрования в компьютерных сетях?

39) Что такое основные протоколы, используемые в Интернет на прикладном уровне? Какие Вы знаете проблемы использования этих протоколов?

40) Что такое характеристика базовых пользовательских технологий: HTTP, FTP, SSH?

41) Что такое сетевая модель OSI? Что такое сеансовый уровень: функции, протоколы?

42) Что такое сетевая модель OSI? Что такое представительский уровень: функции, протоколы?

43) Что такое сетевая модель OSI? Что такое прикладной уровень: функции, протоколы?

44) Что такое протоколы управления SNMP и CMIP?

45) Что такое проксирование трафика?

46) Что такое классификации СОАВ?

47) Какие Вы знаете существующие методы классификации данных в современных СОВ?

48) Какие Вы знаете методы обнаружения ошибок?

49) Какие Вы знаете методы коррекции ошибок?

50) Какие Вы знаете угрозы безопасности информации, передаваемой в локальных сетях ЭВМ?

51) Какие Вы знаете средства контроля внешнего периметра сети?

52) Какие Вы знаете системы трансляции адресов и портов (NAT)?

53) Какие Вы знаете элементы оповещения безопасности систем Dallas Lock?

54) Какие Вы знаете беспроводные технологии передачи данных ?

55) Какие Вы знаете алгоритмы обеспечения безопасности?

56) В чем состоит анализ безопасности существующих протоколов криптографической защиты передачи данных?

57) В чем Ad-hoc? Что такое Manet?

58) Какие Вы знаете алгоритмы безопасной маршрутизации?

6.6 Тематика и содержание курсового проекта

Курсовой проект не предусмотрен.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Пескова, О. Ю. Безопасность сетей ЭВМ : учебное пособие / О. Ю. Пескова, Е. С. Басан ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университет, 2024. - 183 с. - ISBN 978-5-9275-4634-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2180510 (Дата обращения: 26.08.2024). – Режим доступа: по подписке.

2. «Методика оценки угроз безопасности информации», утв. ФСТЭК России 5 февраля 2021 г.: офи- циальный сайт ФСТЭК России [Электронный ресурс] // Режим доступа: https://fstec.ru/tekhni cheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-etodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021) (Дата обращения 26.08.2024).

3. Лозовецкий В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей/ В.В. Лозовецкий, Е.Г. Комаров, В.В. Лебедев: учебное пособие для вузов. - Санкт-Петербург: Лань, 2023. - 488 с. [Электронный ресурс] – Режим доступа: https://e.lanbook.com/book/352292 (дата обращения: 26.08.2024).

4. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю.Н. Сычев. – Москва : ИНФРА-М, 2023 . – 199 с. : ил. + табл. – (Высшее образование: Бакалавриат). – 15 экз.

Дополнительная литература

1. Лабутин Н.Г. Моделирование процессов выявления инцидентов информационной безопасности и реагирования на них / Н.Г. Лабутин, П.В. Костин, Н.Ю. Шадрунова // Труды НГТУ им. Р.Е. Алексеева. 2020. № 4 (131). С. 16-25. [Электронный ресурс]: https://www.elibrary.ru/item.asp?id=44451301 Режим доступа: для авторизованных пользователей (дата обращения: 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. —URL: library.dstu.education.— Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/ .— Текст : электронный.

4. Университетская библиотека онлайн: электронно-библиотечная система. – URL: http://biblioclub.ru/index.php?page=main_ub_red .– Текст : электронный.

5. ЭБС Znanium — URL: http://www.znanium.ru/ . —Текст : электронный.

6. Сайт кафедры ИСИБ http://scs.dstu.education .

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 9.

Таблица 9 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (скамья учебная –20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций:	ауд. *207* корп. *4*
Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС:	ауд. *217* корп. *3* ауд. *211* корп. *4*

Лист согласования РПД

Разработал:
ст. преподаватель кафедры
интеллектуальных систем и
информационной безопасности
(должность)

(подпись) Р.Н. Погорелов
(Ф.И.О.)

И.о. заведующего кафедрой
интеллектуальных систем и
информационной безопасности
(наименование кафедры)

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Протокол № 1 заседания кафедры от 27.08. 2024г.

И.о. декана факультета
информационных технологий
и автоматизации производственных
процессов:
(наименование факультета)

(подпись) В.В. Дьячкова
(Ф.И.О.)

Согласовано

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем

(подпись) Е.Е. Бизянов
(Ф.И.О.)

Начальник учебно-методического центра

(подпись) О.А. Коваленко
(Ф.И.О.)

Лист изменений и дополнений

Номер изменения, дата внесения изменения, номер страницы для внесения изменений	
ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:	ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:
Основание:	
Подпись лица, ответственного за внесение изменений	