

Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Донецкий государственный университет»

Факультет физико-технический
Кафедра радиофизики и инфокоммуникационных технологий



УТВЕРЖДАЮ

проректор

Машу

П.А. Машаров

«29» марта 2024 г.

МП

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ»

Укрупненная группа направлений подготовки	10.00.00 Информационная безопасность
Программа высшего образования	Программа бакалавриат
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Квалификация	Бакалавр
Форма обучения	очная

Рабочая программа адаптирована для лиц
с ограниченными возможностями здоровья и инвалидов

Донецк 2024

Рабочая программа дисциплины «**Защита информации в компьютерных сетях**» для обучающихся по направлению подготовки 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем), составлена на основании Федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427 (с изм. и доп.). Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 06 апреля 2021 г. № 245 (с изм. и доп.), в соответствии с учебным планом, утвержденным Ученым советом ФГБОУ ВО «ДонГУ» для набора 2024 года.

Разработчик:

Ст. преподаватель
кафедры радиофизики
и инфокоммуникационных технологий



Я.И. Рушечников

Рабочая программа утверждена на заседании кафедры радиофизики и инфокоммуникационных технологий
Протокол от 26.03.2024 г. № 16

Заведующий кафедрой



В.В. Данилов

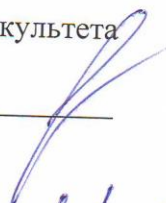
СОГЛАСОВАНО:

И.о. декана физико-технического факультета
28.03.2024 г.



С.А. Фоменко

Учебно-методическая комиссия физико-технического факультета
Протокол от 27.03.2024 г. № 2
Председатель



В. Н. Котенко

Руководитель основной профессиональной
образовательной программы
д-р тех. наук, проф.
26.03.2024 г.



В.В. Данилов

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Требования к предварительной подготовке обучающихся, предшествующие и сопутствующие дисциплины, на которых основывается изучение данной:

дисциплины программы бакалавриата: Информатика, Дискретная математика, Архитектура компьютерных систем, Модели и методы безопасного информационного обмена.

1.2. Дисциплины, курсовые работы и практики, для которых освоение данной дисциплины необходимо как предшествующее:

Защита информации в виртуальных сетях, является основой для прохождения практик; используются при подготовке выпускной квалификационной работы.

2. ОПИСАНИЕ ДИСЦИПЛИНЫ

2.1. Общая характеристика

Наименование показателя	Значение показателя
Название образовательной программы	10.03.01 Информационная безопасность (Программа бакалавриата: 10.03.01 Информационная безопасность (Профиль: Безопасность автоматизированных систем))
Шифр и название в соответствии с учебным планом	Б1.В.ДВ.6.1. Защита информации в компьютерных сетях
Часть образовательной программы	Вариативная часть: выбор обучающегося
Количество зачетных единиц / всего часов	4 / 144

2.2. Распределение часов по формам и периодам обучения

Форма обучения	курс	семестр	Общее количество часов					Форма контроля
			лекционных	лабораторных	практических	самостоятельной работы + контроль	всего	
Очная, всего	3	5	34	34	-	76	144	экзамен

3. ЦЕЛИ ДИСЦИПЛИНЫ

Изучение уязвимостей в современных компьютерных сетях, а также средств обеспечения сетевой безопасности, которые нивелируют эти уязвимости.

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ КОМПОНЕНТА ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ, ИХ ИНДИКАТОРЫ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

4.1. Компетенции

Компетенции	Индикаторы	Результаты обучения
ПК-1. Способен выполнять администрирование средств защиты информации в компьютерных сетях.	ПК-1.1. Умеет выполнять администрирование средств защиты информации в компьютерных сетях.	ПК-1.1.1. Знает методы обработки информации с использованием современных технических средств коммуникации и связи. ПК-1.1.2. Знает современные программные средства системного и прикладного

		<p>назначения отечественного и российского производства.</p> <p>ПК-1.1.3. Умеет использовать современные программные средства системного и прикладного назначения для решения задач информационной безопасности.</p>
--	--	--

5. ПРОГРАММА ДИСЦИПЛИНЫ

Название темы	Краткое содержание темы (вопросы темы)
Тема 1. Компьютерные сети и сетевая безопасность.	<p>1.1. Компьютерная сеть, как цель для злоумышленника.</p> <p>1.2. Классификация компьютерных сетей.</p> <p>1.3. Необходимость обеспечения сетевой безопасности.</p> <p>1.4. Облачные и виртуальные сети.</p> <p>1.5. Расширение границы сети.</p> <p>1.6. Краткая информация об инструментах проведения атак.</p> <p>1.7. Организации, которые формируют стандарты в сфере защиты информации в компьютерных сетях.</p>
Тема 2. Обеспечение безопасности сетевых устройств.	<p>2.1. Защита сетевой инфраструктуры.</p> <p>2.2. Подходы к защите граничных маршрутизаторов.</p> <p>2.3. Три области защиты маршрутизатора.</p> <p>2.4. Обеспечение защиты административного доступа.</p> <p>2.5. Безопасный локальный и удаленный доступ.</p> <p>2.6. Усовершенствование процесса входа в систему.</p> <p>2.7. Протокол SSH.</p> <p>2.8. Назначение административных ролей.</p> <p>2.9. 16 уровней привилегий в сетевом оборудовании Cisco.</p> <p>2.10. Ограничения уровней привилегий.</p> <p>2.11. Функция устойчивой конфигурации Cisco IOS.</p> <p>2.12. Основные сведения о системном журнале.</p> <p>2.13. Основные сведения о протоколе SNMP.</p> <p>2.14. Уязвимости SNMP.</p> <p>2.15. Протокол сетевого времени.</p> <p>2.16. Уязвимости плоскостей управления и менеджмента.</p>
Тема 3. Аутентификация, авторизация и учет.	<p>3.1. Компоненты AAA.</p> <p>3.2. Локальная аутентификация.</p> <p>3.3. Серверная аутентификация.</p> <p>3.4. Авторизация.</p> <p>3.5. Учет.</p> <p>3.6. Протоколы TACACS+ и RADIUS.</p> <p>3.7. Мониторинг трафика аутентификации.</p> <p>3.8. Обеспечение безопасности с использованием аутентификации 802.1X на основе портов.</p>
Тема 4. Внедрение технологий межсетевого экрана.	<p>4.1. Настройка нумерованных и именованных списков ACL.</p> <p>4.2. Правила настройки списка ACL.</p> <p>4.3. Защита от спуфинга с помощью списков ACL.</p> <p>4.4. Сведения о списках ACL для IPv6.</p> <p>4.5. Принцип работы межсетевого экрана.</p> <p>4.6. Преимущества и ограничения межсетевых экранов.</p>

	<p>4.7. Описание типов межсетевых экранов.</p> <p>4.8. Преимущества и ограничения межсетевых экранов с фильтрацией пакетов.</p> <p>4.9. Принцип работы классического межсетевого экрана. Внутренние и внешние сети.</p> <p>4.10. Демилитаризованные зоны.</p> <p>4.11. Практические рекомендации для межсетевого экрана.</p>
Тема 5. Внедрение системы предотвращения вторжений.	<p>5.1. 0 day Атаки.</p> <p>5.2. Обнаружение и остановка атак.</p> <p>5.3. Мониторинг атак.</p> <p>5.4. Преимущества и недостатки систем IDS и IPS.</p> <p>5.5. Хостовая реализация IPS.</p> <p>5.6. Сетевые IPS-сенсоры.</p> <p>5.7. Выбор решения IPS.</p> <p>5.8. Атрибуты сигнатур.</p> <p>5.9. Файл сигнатур.</p> <p>5.10. Сигнал тревоги сигнатуры.</p> <p>5.11. Действия сигнатур.</p> <p>5.11. Мониторинг активности.</p>
Тема 6. Обеспечение безопасности локальной сети.	<p>6.1. Обеспечение защиты элементов LAN.</p> <p>6.2. Обеспечение безопасности оконечных устройств традиционным способом.</p> <p>6.3. Локальная сеть в нынешних реалиях.</p> <p>6.4. Вопросы обеспечения безопасности в сетях нового типа.</p> <p>6.5. Современные решения для безопасности оконечных устройств.</p> <p>6.6. AMP, Advanced Malware Protection.</p> <p>6.7. Форматы AMP по мету применения.</p> <p>6.8. Устройство защиты электронной почты ESA.</p> <p>6.9. Устройство защиты web трафика WSA.</p> <p>6.10. Решения для контроля доступа к сети.</p> <p>6.11. Описание уязвимостей на 2-м уровне.</p> <p>6.12. Атака на таблицу CAM.</p> <p>6.13. Инструменты атаки на таблицу CAM.</p> <p>6.14. Спуфинг адресов.</p>
Тема 7. Внедрение виртуальных частных сетей.	<p>7.1. Знакомство с сетями VPN.</p> <p>7.2. Преимущества VPN.</p> <p>7.3. Сети IPsec VPN 3-го уровня.</p> <p>7.4. Типы сетей VPN.</p> <p>7.5. Компоненты сетей VPN между двумя пунктами.</p> <p>7.6. Разворот пакетов (Hairpinning) и разделенное туннелирование (Split Tunneling).</p> <p>7.7. Безопасный обмен ключами.</p> <p>7.8. Основные возможности pfSense.</p>
Тема 8. Безопасность беспроводных сетей.	<p>8.1. Распределение частот по индивидуальным каналам в диапазоне 2.4 ГГц.</p> <p>8.2. Частоты каналов.</p> <p>8.3. Технология MIMO.</p> <p>8.4. Режимы работы беспроводных сетей.</p> <p>8.5. Основные режимы работы сетей Wi-Fi.</p> <p>8.6. Контроллер беспроводной сети.</p> <p>8.7. 5 главных целей злоумышленника.</p>

	8.8. Атаки на контроль доступа. 8.9. Атаки на конфиденциальность. 8.10. DoS. 8.11. Атаки поддельной точки доступа. 8.12. Атаки перелокации клиента. 8.13. Атаки на неправильную настройку точки доступа. 8.14. Как обезопасить беспроводную сеть.
--	---

6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

6.1. Форма обучения – очная, курс – 3, семестр – 5

Наименования разделов и тем	Количество часов				
	Лекц.	Лабор.	Практ.	СРС+К	Всего
Тема 1. Компьютерные сети и сетевая безопасность.	4	4	-	9	17
Тема 2. Обеспечение безопасности сетевых устройств.	4	4	-	9	17
Тема 3. Аутентификация, авторизация и учет.	4	4	-	9	17
Тема 4. Внедрение технологий межсетевого экрана.	4	4	-	9	17
Тема 5. Внедрение системы предотвращения вторжений.	4	4	-	10	18
Тема 6. Обеспечение безопасности локальной сети.	5	5	-	10	20
Тема 7. Внедрение виртуальных частных сетей.	5	5	-	10	20
Тема 8. Безопасность беспроводных сетей.	4	4	-	10	18
ИТОГО ПО КОМПОНЕНТУ ОПОП	34	34	-	76	144

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (СРЕДСТВА) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Контрольные вопросы

1. Что такое компьютерная сеть.
2. Какая на ваш взгляд модель является более практичной: TCP/IP или ISO/OSI.
3. Что такое сетевой пакет?
4. Сетевой пакет и сетевой кадр, в чём отличия.
5. Транспортный уровень КС. Протоколы транспортного уровня.
6. Сетевые топологии и их уязвимости.
7. Что такое маршрутизация. Протоколы маршрутизации.
8. Что такое IP адрес и для чего нужна маска.
9. Особые IP-адреса. Понятие частных сетей. Диапазоны частных адресов.
10. Адресация IPv6. Особенности.
11. Какие задачи позволяет решать анализатор (Сниффер).
12. Для чего нужны фильтры? Приведите пример из программирования, который похож на фильтры.
13. В чём разница между фильтрами захвата и отображения?
14. Для чего нужен неразборчивый режим (Promiscuous mode).
15. Что такое сканирование.
16. Какие цели у сканирования.

17. К каким типам атак относится сканирование.
18. Для чего нужна параллельная обработка в NMAP.
19. Что такое профили сканирования и для чего они нужны.
20. Каким образом можно обнаружить сканирование в сети.
21. Как можно обнаружить сниффер в сети.
22. Что нужно предпринимать при обнаружении сканирования или прослушивания сети.
23. Что такое Scapy.
24. Механизмы взаимодействия со Scapy.
25. Основные возможности Scapy.

7.2. Темы докладов

1. Сетевой сканер Nessus.
2. Ханипоты и их применение.
3. Системы серверной аутентификации.
4. Snort как система обнаружения вторжений.
5. Трояны удалённого доступа.
6. Системы безопасного сетевого туннелирования.
7. Специальные уязвимые системы для тренировки навыков специалиста ИБ.
8. Социоинженерные сетевые системы.

7.3. Образец содержания экзаменационного билета (при наличии экзамена по дисциплине)

В случае ведения учебного процесса с использованием электронного обучения и дистанционных образовательных технологий, содержание билета может отличаться от приведенного.

ОБРАЗЕЦ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Донецкий государственный университет

Физико-технический факультет

Кафедра радиофизики и инфокоммуникационных технологий

Программа высшего образования	Программа бакалавриата
Направление подготовки	10.03.01 Информационная безопасность
Профиль подготовки	Безопасность автоматизированных систем
Форма обучения	Очная
Семестр	Шестой
Дисциплина	Защита информации в компьютерных сетях

Экзаменационный билет № 1

1. Для чего нужна параллельная обработка в NMAP.
2. Что такое маршрутизация. Протоколы маршрутизации.
3. Для чего нужны фильтры? Приведите пример из программирования, который похож на фильтры.

Утверждено на заседании кафедры радиофизики и инфокоммуникационных технологий, протокол № __ от __.__.202__ г.

Заведующий кафедрой

В.В. Данилов

Экзаменатор

Я.И. Рушечников

8. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Общая оценка знаний обучающихся по дисциплине проводится по 100-балльной шкале исходя из максимума, приведенного в таблице ниже. Организационно-учебная работа в аудитории оценивается на основе таких критериев как посещаемость занятий, своевременное и качественное выполнение домашних заданий, активность во время проведения лекционных и практических занятий (участие в обсуждении текущего и пройденного материала, решение задач и т.п.).

8.1. Семестр 1

Номера разделов	Виды работ	Максимальное количество баллов
1-8	Организационно-учебная работа обучающегося в аудитории	30
	Самостоятельная работа	20
	Модульная контрольная работа	10
ИТОГО		60
Экзамен		40
Общий итог за семестр		100

Соответствие баллов оценке

Количество баллов из 100	ECTS	Оценка по пятибалльной шкале	
		Экзамен, дифференцированный зачет	Зачет
90-100	A	отлично	зачтено
80-89	B	хорошо	зачтено
75-79	C		зачтено
70-74	D	удовлетворительно	зачтено
60-69	E		зачтено
35-59	FX	неудовлетворительно	не зачтено
0-34	F		не зачтено

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

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

- 1) для слепых и слабовидящих:
 - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
 - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
 - письменные задания оформляются увеличенным шрифтом.
- 2) для глухих и слабослышащих:
 - лекции оформляются в виде электронного документа;
 - письменные задания выполняются на компьютере в письменной форме;
 - экзамен проводится в письменной форме на компьютере; возможно проведение в форме тестирования.
- 3) 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;
- 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.

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:

- 1) для слепых и слабовидящих:
 - в печатной форме увеличенным шрифтом;
 - в форме электронного документа;
- 2) для глухих и слабослышащих:
 - в печатной форме;
 - в форме электронного документа.
- 3) для обучающихся с нарушениями опорно-двигательного аппарата:
 - в печатной форме;
 - в форме электронного документа.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

Учебные занятия проводятся в корпусе №4 ДонГУ (г. Донецк, пр. Театральный, 13). Для проведения лекционных занятий требуется аудитория, оборудованная меловой или маркерной доской, мультимедийный проектор и экран, ноутбук, комплект учебной мебели для студентов, рабочее место преподавателя, выход в Интернет – проводной или с использованием Wi-Fi.

Для проведения лабораторных занятий требуется оборудованная персональными компьютерами аудитория.

Для самостоятельной работы используются текстовые и электронные ресурсы Научной библиотеки университета и других электронных библиотечных баз данных, учебно-методическое обеспечение, представленное в учебно-методическом кабинете Главного корпуса (ауд.405).

Обучающиеся имеют возможность использовать учебные материалы по дисциплине, размещенные на платформе Moodle Центра дистанционного образования ФГБОУ ВО «ДонГУ». При изучении дисциплины применяются электронное обучение и дистанционные образовательные технологии.

С использованием ресурсов платформы дистанционного образования осуществляется текущий контроль знаний обучающихся на основе тестирования и проверки результатов самостоятельной работы.

11. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

11.1. Основная литература

1. Таненбаум Э. Компьютерные сети. Шестое издание. Э.Таненбаум. Х.Бос - Санкт-Петербург 2019- 978-5-4461-1766-6

11.2. Дополнительная литература

2. Таненбаум Э. Современные операционные системы. Э.Таненбаум. Х.Бос - Санкт-Петербург 2017 - 978-5-4461-1155-8.

12. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. Научная электронная библиотека elibrary.ru : информ.-аналит. портал / ООО Научная электронная библиотека. – Москва : ООО Науч. электрон. б-ка, сор. 2000–2022. – URL: <https://elibrary.ru> (дата обращения: 01.01.2024). – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. Электронный каталог Научной библиотеки Донецкого государственного университета. – Донецк : НБ ДонГУ, 1999– . – URL: <http://catalog.donnu.education> (дата обращения: 01.01.2024). – Текст : электронный;

3. Учебники и другие книги по математике URL: <http://eqworld.ipmnet.ru/ru/library/mathematics.htm> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный

4. Интернет-библиотека Виталия Арнольда URL: <http://ilib.mcsme.ru/> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный;

5. Техническая библиотека URL: <http://techlibrary.ru/> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный;

6. Научные журналы ФГБОУ ВО «ДонГУ» URL: <http://donnu.ru/science/journals> (дата обращения: 31.03.2024). – Режим доступа: свободный. – Текст : электронный.

13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Windows 7 PRO (корпоративная лицензия ДонГУ № 46484614)
2. Microsoft Office (корпоративная лицензия ДонГУ № 46472919)
3. Microsoft Visual Studio (лицензия программы Dream Spark для высших учебных заведений)
4. Система виртуализации Oracle VirtualBox (свободно распространяемая)
5. Антивирус Касперского, Adobe Acrobat Reader, xPDF (лицензии GPL, Apache, BSD для свободного программного обеспечения).