Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

Факультет физико-математических и естественных наук
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

02.04.02 ФУНДАМЕНТАЛЬНАЯ ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

БЕСПРОВОДНЫЕ СЕТИ, ИНТЕРНЕТ ВЕЩЕЙ И КИБЕРБЕЗОПАСНОСТЬ
(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Обеспечение безопасности в сетях передачи данных» входит в программу магистратуры «Беспроводные сети, интернет вещей и кибербезопасность» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается во 2 семестре 1 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 7 разделов и 17 тем и направлена на изучение протоколов безопасности, способов мониторинга и аудита сетей передачи данных.

Целью освоения дисциплины является изучение протоколов, методов мониторинга и аудита безопасности сетей передачи данных, в том числе специализированных.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Обеспечение безопасности в сетях передачи данных» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
ПК-3	Проведение анализа безопасности компьютерных систем	ПК-3.1 Знает уязвимости компьютерных систем и сетей; ПК-3.4 Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия; ПК-3.5 Умеет разрабатывать предложения по устранению выявленных уязвимостей; ПК-3.6 Умеет составлять и оформлять аналитический отчет по результатам проведенного анализа;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Обеспечение безопасности в сетях передачи данных» относится к блоку по выбору блока образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Обеспечение безопасности в сетях передачи данных».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ПК-3	Проведение анализа безопасности компьютерных систем		Моделирование угроз кибербезопасности; Статистическое моделирование в кибербезопасности; Преддипломная практика;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Обеспечение безопасности в сетях передачи данных» составляет «4» зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			2
Контактная работа, ак.ч.	*36*		*36*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	18		18
Самостоятельная работа обучающихся, ак.ч.	*108*		*108*
Контроль (экзамен/зачет с оценкой), ак.ч.	*0*		*0*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Основы сетей передачи данных	1.1	Принципы построения сетей передачи данных (PDH, SDH, OTN, IP/MPLS)	ЛК, СЗ
		1.2	Классификация сетей (WAN, MAN, LAN, PAN) и их особенности	ЛК, СЗ
		1.3	Стандарты и протоколы передачи данных (IEEE, ITU-T, IETF): IEEE 802.1X, IEEE 802.1Q, ITU-T X.200, ITU-T Q.931, RFC 791, RFC 2460, RFC 4364	ЛК, СЗ
Раздел 2	Основы архитектуры и принципов безопасности СПД	2.1	Архитектурные подходы к обеспечению безопасности СПД - Зонирование и сегментация сетей. - Иерархическая организация СПД. - Роль межсетевых экранов (firewalls) и маршрутизаторов.	ЛК, СЗ
		2.2	Протоколы и стандарты безопасности в СПД - Анализ протоколов IPsec, MPLS, VLAN. - Безопасность в технологии SDN (Software-Defined Networking).	ЛК, СЗ
Раздел 3	Управление доступом и контроль трафика	3.1	Системы управления доступом в СПД - Методы аутентификации устройств и пользователей. - Политики контроля доступа (ACL, RBAC). - Безопасность в беспроводных сетях (Wi-Fi, LTE, 5G).	ЛК, СЗ
		3.2	Фильтрация и управление трафиком - Технологии фильтрации пакетов и потоков данных. - Принципы работы Deep Packet Inspection (DPI).	ЛК, СЗ
Раздел 4	Безопасность протоколов и технологий СПД	4.1	Безопасность сетевых протоколов - Анализ уязвимостей протоколов BGP, DNS, DHCP. - Безопасность в IPv6.	ЛК, СЗ
		4.2	Безопасность виртуальных сетей - Принципы организации Virtual Private Networks (VPN). - Безопасность в технологиях виртуализации сетей (NFV, VPLS).	ЛК, СЗ
Раздел 5	Мониторинг и аудит безопасности СПД	5.1	Методы мониторинга сетей передачи данных - Принципы работы систем IDS и IPS. - Мониторинг сетевого трафика с использованием SIEM-систем.	ЛК, СЗ
		5.2	Аудит и тестирование безопасности СПД - Методологии проведения аудита безопасности. - Проверка соответствия стандартам (ISO/IEC 27001).	ЛК, СЗ
Раздел 6	Особенности безопасности специализированных СПД	6.1	Безопасность IoT-сетей - Особенности защиты сетей Интернета вещей (IoT). - Проблемы масштабируемости и изоляции устройств.	ЛК, СЗ
		6.2	Безопасность промышленных сетей передачи данных	ЛК, СЗ
Раздел 7	Особенности безопасности	7.1	Теоретические основы применения ИИ в защите сетей	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
	специализированных СПД	7.2	Автоматизация обнаружения угроз с помощью ИИ	ЛК, СЗ
		7.3	Использование ИИ для управления безопасностью	ЛК, СЗ
		7.4	Ограничения и вызовы использования ИИ в защите сетей. Проблемы качества данных и adversarial attacks.	ЛК, СЗ

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.*

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или ЯндексТелемост.
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или ЯндексТелемост,Anaconda Navigator, Spyder,python
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или ЯндексТелемост.

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО**!

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Сети и телекоммуникации : учебник и практикум для вузов / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва :

Издательство Юрайт, 2025. — 464 с. — (Высшее образование). — ISBN 978-5-534-17315-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560392

2. Comer, D. E. Internetworking with TCP/IP: Principles, Protocols, and Architecture / D. E. Comer. — 6th ed. — Pearson, 2022. — 768 p.

3. Freeman, R. Telecommunication System Engineering / R. Freeman. — 5th ed. — Wiley, 2022. — 500 p.

4. Stallings, W. Data and Computer Communications / W. Stallings. — 11th ed. — Pearson, 2022. — 900 p.

5. IEEE 802 Standards Collection: Overview and Architecture. — IEEE Standards Association, 2022.

6. ITU-T Recommendation G.709: Interface for the Optical Transport Network (OTN). — Geneva: International Telecommunication Union, 2021.

7. Stallings, W. Network Security Essentials: Applications and Standards / W. Stallings. — 7th ed. — Pearson, 2021. — 464 p.

8. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. — 3rd ed. — Wiley, 2021. — 848 p.

9. Scarfone, K. Guide to Intrusion Detection and Prevention Systems (IDPS) / K. Scarfone, P. Mell. — NIST Special Publication 800-94, 2022. — 120 p.

10. ISO/IEC 27001:2022: Information Security Management / ISO. — Geneva: International Organization for Standardization, 2022.

11. Kreibich, J. Network Programmability and Automation / J. Kreibich, M. Birkholz, T. Graf. — O'Reilly Media, 2021. — 400 p.

12. Stouffer, K. Guide to Industrial Control Systems (ICS) Security / K. Stouffer, J. Falco, K. Scarfone. — NIST Special Publication 800-82, 2021. — 200 p.

13. Kreutz, D. Software-Defined Networking: A Comprehensive Survey / D. Kreutz, F. M. V. Ramos, P. E. Verissimo // Proceedings of the IEEE. — 2022. — Vol. 110, No. 1. — P. 1–25.

14. Stallings, W. Wireless Communications & Networks / W. Stallings. — 3rd ed. — Pearson, 2022. — 550 p.

15. Chowdhury, N. M. A Survey of Network Virtualization / N. M. Chowdhury, R. Boutaba // Computer Networks. — 2022. — Vol. 200. — P. 108–120.

16. Roman, R. On the Features and Challenges of Security and Privacy in Distributed Internet of Things / R. Roman, J. Zhou, J. Lopez // Future Generation Computer Systems. — 2021. — Vol. 115. — P. 45–60.

Дополнительная литература:

1. Huitema, C. IPv6 Essentials / C. Huitema. — 4th ed. — O'Reilly Media, 2021. — 350 p.

2. RFC 7916: Operational Security Considerations for IPv6 Networks / IETF. — 2021.

3. RFC 8576: Internet of Things (IoT) Security: Review and Challenges / IETF. — 2021.

4. RFC 9064: Guidelines for Operating SCADA Systems in Critical Infrastructure / IETF. — 2021.

5. Ferguson, P. IP Multicast with Applications to MPLS VPNs and Network Security / P. Ferguson, G. Huston. — Cisco Press, 2021. — 300 p.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН https://mega.rudn.ru/MegaPro/Web
- ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru
- ЭБС «Юрайт» http://www.biblio-online.ru
- ЭБС «Консультант студента» www.studentlibrary.ru

- ЭБС «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы

- Sage https://journals.sagepub.com/
- Springer Nature Link https://link.springer.com/
- Wiley Journal Database https://onlinelibrary.wiley.com/
- Наукометрическая база данных Lens.org https://www.lens.org

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Обеспечение безопасности в сетях передачи данных».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС**!

РАЗРАБОТЧИК:

Доцент кафедры теории вероятностей и кибербезопасности		Ботвинко Анатолий Юрьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*