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

ИСТОЧНИКИ УГРОЗ КИБЕРБЕЗОПАСНОСТИ И АНАЛИЗ УЯЗВИМОСТЕЙ

(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 «Источники угроз кибербезопасности и анализ уязвимостей» входит в программу магистратуры «Беспроводные сети, интернет вещей и кибербезопасность» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается в 1 семестре 1 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 5 разделов и 20 тем и направлена на изучение и анализ уязвимостей в киберфизических системах.

Целью освоения дисциплины является знакомство обучающихся с источниками угроз, их классификацией и типизацией, с методологией анализа уязвиместей в различных киберфизических системах.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Источники угроз кибербезопасности и анализ уязвимостей» 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)
ОПК-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1 Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла; ОПК-4.2 Умеет осуществлять управление проектами информационных систем; ОПК-4.3 Имеет практический опыт анализа и интерпретации информационных систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Источники угроз кибербезопасности и анализ уязвимостей» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Источники угроз кибербезопасности и анализ уязвимостей».

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

Шифр	**Наименование компетенции**	**Предшествующие дисциплины/модули, практики***	**Последующие дисциплины/модули, практики***
ОПК-4	Способен оптимальным образом комбинировать существующие информационно-коммуникационные		Криптографические методы защиты информации; Анализ и показатели эффективности кибербезопасности

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности		предприятия; Технологическая (проектно-технологическая) практика; Научно-исследовательская работа;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Источники угроз кибербезопасности и анализ уязвимостей» 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)**
			1
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.	*81*		*81*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
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	Нормативно-правовые и организационные основы анализа уязвимостей	1.1	Основные понятия и термины	ЛК, СЗ
		1.2	Международные стандарты и требования по анализу уязвимостей	ЛК, СЗ
		1.3	Международные регламенты и рекомендации по анализу уязвимостей	ЛК, СЗ
		1.4	Стандарты и нормативные требования Российской Федерации по анализу уязвимостей	ЛК, СЗ
		1.5	Базы данных и инструменты поиска уязвимостей Российской Федерации	ЛК, СЗ
Раздел 2	Классификация источников угроз и уязвимостей	2.1	Источники угроз	ЛК, СЗ
		2.2	Классификации угроз	ЛК, СЗ
		2.3	Типы уязвимостей	ЛК, СЗ
Раздел 3	Методологии анализа уязвимостей	3.1	Статический анализ уязвимостей	ЛК, СЗ
		3.2	Динамический анализ уязвимостей. Фаззинг и символьное исполнение	ЛК, СЗ
		3.3	Сравнительный анализ существующих методологий анализа уязвимостей	ЛК, СЗ
Раздел 4	Математические основы анализа уязвимостей	4.1	Теория графов в моделировании атак. Деревья атак, деревья атак (Attack Trees), визуализация возможных векторов атак	ЛК, СЗ
		4.2	Система оценки уязвимостей CVSS (Common Vulnerability Scoring System)	ЛК, СЗ
		4.3	Прогнозирования вероятности эксплуатации уязвимости с помощью методологии EPSS (Exploitability, Prevalence, and Severity Score)	ЛК, СЗ
Раздел 5	Современные и перспективные угрозы кибербезопасности	5.1	Уязвимости в IoT и киберфизических системах	ЛК, СЗ
		5.2	Уязвимости в облачных средах	ЛК, СЗ
		5.3	Уязвимости в системах машинного обучения и ИИ	ЛК, СЗ
		5.4	Правовые основы применения технологий искусственного интеллекта в сфере информационной безопасности в Российской Федерации	ЛК, СЗ
		5.5	Угрозы безопасности информации, связанные с технологиями искусственного интеллекта	ЛК, СЗ
		5.6	Искусственный интеллект в анализе уязвимостей	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;	Компьютер/ноутбук с доступом сети Интернет и электронно-

	доской (экраном) и техническими средствами мультимедиа презентаций.	образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или ЯндексТелемост, Anaconda Navigator, Spyder, Python
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. Бирюков А.А. Информационная безопасность. Защита и нападение. - 2-е изд. - М.: ДМК Пресс, 2022. - 320 с.

2. Диогенес Ю., Озкая Э. Кибербезопасность: стратегии атак и обороны. - СПб.: Питер, 2021. - 416 с.

3. Яворски П. Ловушка для багов: Практическое руководство по поиску уязвимостей. - М.: Альпина Паблишер, 2023. - 280 с.

4. Замм А. и др. Kali Linux. Тестирование на проникновение. - М.: БХВ-Петербург, 2023. - 480 с.

Дополнительная литература:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 24.02.2021)

2. Приказ ФСТЭК России от 25.12.2020 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов КИИ»

3. ГОСТ Р 57580.1-2021 «Безопасность финансовых организаций. Требования к защите информации»

4. NIST SP 800-53 Rev. 5 (2021) «Security and Privacy Controls for Information Systems»

5. CI DSS v4.0 (2022) «Payment Card Industry Data Security Standard»

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 «Источники угроз кибербезопасности и анализ уязвимостей».

* - 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.*