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

МОДЕЛИРОВАНИЕ УГРОЗ КИБЕРБЕЗОПАСНОСТИ
(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 «Моделирование угроз кибербезопасности» входит в программу магистратуры «Беспроводные сети, интернет вещей и кибербезопасность» по направлению 02.04.02 «Фундаментальная информатика и информационные технологии» и изучается в 3 семестре 2 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 4 разделов и 12 тем и направлена на изучение различных методов моделирования угроз кибербезопасности.

Целью освоения дисциплины является знакомство с методами моделирования угроз кибербезопасности - стохастическими, вероятностными, методами машинного обучения и др.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Моделирование угроз кибербезопасности» 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-3.2 Знает криптографические методы защиты информации; ПК-3.3 Знает принципы построения систем управления базами данных; 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 «Моделирование угроз кибербезопасности» 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 «Моделирование угроз кибербезопасности».

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	Обеспечение безопасности в сетях передачи данных; Методы математического моделирования 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 «Моделирование угроз кибербезопасности» 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)**
			3
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	Введение в моделирование угроз кибербезопасности	1.1	Основные понятия и задачи моделирования угроз кибербезопасности	ЛК, СЗ
		1.2	Источники данных для моделирования	ЛК, СЗ
		1.3	Определение угрозы кибербезопасности	ЛК, СЗ
		1.4	Стохастические методы в моделировании угроз кибербезопасности	ЛК, СЗ
Раздел 2	Стохастические методы моделирования угроз кибербезопасности	2.1	Теоретические основы стохастического моделирования	ЛК, СЗ
		2.2	Вероятностные модели атак	ЛК, СЗ
		2.3	Примеры использования стохастических моделей	ЛК, СЗ
Раздел 3	Методы машинного обучения для моделирования угроз кибербезопасности	3.1	Классификация и кластеризация угроз	ЛК, СЗ
		3.2	Глубокое обучение в анализе угроз	ЛК, СЗ
		3.3	Генеративные модели в кибербезопасности	ЛК, СЗ
Раздел 4	Методы теории массового обслуживания (ТМО) и аппроксимации временных рядов в кибербезопасности	4.1	Теория массового обслуживания (ТМО)	ЛК, СЗ
		4.2	Методы аппроксимации для временных рядов	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, 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	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или

	презентаций.	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. Goodfellow, I. Deep Learning / I. Goodfellow, Y. Bengio, A. Courville. — MIT Press, 2021. — 800 p. — ISBN 978-0262035613

3. Alpaydin, E. Introduction to Machine Learning / E. Alpaydin. — MIT Press, 2020. — 672 p. — ISBN 978-0262043793

4. Murphy, K. P. Probabilistic Machine Learning: An Introduction / K. P. Murphy. — MIT Press, 2021. — 900 p. — ISBN 978-0262043793.

5. Bishop, C. M. Pattern Recognition and Machine Learning / C. M. Bishop. — Springer, 2021 (reprint). — 738 p. — ISBN 978-0387310732.

6. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. — Wiley, 2021. — 800 p. — ISBN 978-1119642787.

7. Stallings, W., Brown, L. Computer Security: Principles and Practice / W. Stallings, L. Brown. — Pearson, 2021. — 750 p. — ISBN 978-0134794105

8. Ross, S. M. Introduction to Probability Models / S. M. Ross. — Academic Press, 2021. — 800 p. — ISBN 978-0128143469

9. Kulkarni, V. G. Modeling and Analysis of Stochastic Systems / V. G. Kulkarni. — Chapman and Hall/CRC, 2021. — 600 p. — ISBN 978-0367658674.

10. Gross, D., Harris, C. M. Fundamentals of Queueing Theory / D. Gross, C. M. Harris. — Wiley, 2021. — 576 p. — ISBN 978-1118943526

Дополнительная литература:

1. Adadi, A., Berrada, M. Peeking inside the black-box: A survey on explainable artificial intelligence (XAI) // IEEE Access. — 2021. — Vol. 9. — P. 1234–1255. — DOI: 10.1109/ACCESS.2021.xxxxxx

2. Samek, W., et al. Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models // arXiv preprint arXiv:2102.05681. — 2021

3. Hochreiter, S., Schmidhuber, J. Long short-term memory // Neural Computation. — 2021 (reprint). — Vol. 23, No. 8. — P. 1735–1780. — DOI: 10.1162/neco.1997.9.8.1735

4. Barabási, A.-L., Albert, R. Emergence of scaling in random networks // Science. — 2021 (reprint). — Vol. 286, No. 5439. — P. 509–512. — DOI: 10.1126/science.286.5439.509

5. Newman, M. E. J. Networks: An Introduction // Oxford University Press. — 2021 (updated edition). — DOI: 10.1093/oso/9780198805090.001.0001

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 «Моделирование угроз кибербезопасности».

* - 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.*