

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 26.05.2026 14:43:36

Уникальный программный ключ:

ca953a01204891083f939673076ef1a989dae18a

**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**

### **МЕТОДЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ В 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)

**2026 г.**

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Методы математического моделирования в кибербезопасности» 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 4 разделов и 8 тем и направлена на изучение математических основ защиты информации, моделирования кибератак и угроз, прогнозирования и предотвращения угроз.

Целью освоения дисциплины является освоение инструментов для анализа и прогнозирования киберугроз с использованием математических подходов. Дисциплина готовит специалистов к проектированию систем защиты, способных адаптироваться к динамичным угрозам, и формирует навыки работы с инструментами анализа данных, криптографии и прогнозного моделирования.

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Методы математического моделирования в 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-1	Проведение работ по обработке и анализу научно-технической информации и результатов исследований	ПК-1.1 Знает основы научно-исследовательской деятельности в области информационных технологий; владеет знанием основ философии и методологии науки; владеет методами научных исследований, умеет применять их на практике; ПК-1.2 Знает принципы построения научной работы, методы сбора и анализа полученного материала, способы аргументации; владеет навыками подготовки научных обзоров, публикаций, рефератов и библиографий по тематике проводимых исследований на русском и иностранном языке; способен готовить публикации в научно-технических тематических изданиях; ПК-1.3 Умеет применять полученные знания в области фундаментальных научных основ математики и информатики, а также решать стандартные задачи собственной научно-исследовательской деятельности; умеет решать научные задачи с пониманием существующих подходов к верификации моделей по тематике исследований в соответствии с выбранной методикой; ПК-1.4 Знает основы ведения научной дискуссии и формы устного научного высказывания; умеет вести корректную дискуссию в области информационных технологий, задавать вопросы и отвечать на поставленные вопросы по теме научного исследования; владеет навыками выступлений и научной аргументации при анализе объекта научной и профессиональной деятельности; способен принимать участие в работе научных семинаров, научно-технических конференций;
ПК-3	Проведение анализа безопасности компьютерных систем	ПК-3.4 Умеет анализировать компьютерную систему с целью определения уровня защищенности и доверия; ПК-3.6 Умеет составлять и оформлять аналитический отчет по результатам проведенного анализа; ПК-3.7 Знает и применяет методики описания и

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		моделирования бизнес-процессов; средства моделирования бизнес-процессов; основы реинжиниринга бизнес-процессов организации; ПК-3.8 Проводит анализ требований к системе; проводит оценку качества, надежности и эффективности системы;

### 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Методы математического моделирования в 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 «Методы математического моделирования в 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-1	Проведение работ по обработке и анализу научно-технической информации и результатов исследований		Преддипломная практика; Научно-исследовательская работа; Показатели эффективности беспроводных сетей последующих поколений; Computer Skills for Scientific Writing; Карта бизнес-процессов и информационная модель управления телекоммуникациями;
ПК-3	Проведение анализа безопасности компьютерных систем		Моделирование угроз кибербезопасности; Статистическое моделирование в кибербезопасности; Карта бизнес-процессов и информационная модель управления телекоммуникациями; Показатели эффективности беспроводных сетей последующих поколений; 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 «Методы математического моделирования в 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)
			2
<i>Контактная работа, ак.ч.</i>	54		54
Лекции (ЛК)	18		18
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	36		36
<i>Самостоятельная работа обучающихся, ак.ч.</i>	63		63
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	27		27
<b>Общая трудоемкость дисциплины</b>	<b>ак.ч.</b>	<b>144</b>	<b>144</b>
	<b>зач.ед.</b>	<b>4</b>	<b>4</b>

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Основы математического моделирования	1.1	Математический аппарат моделирования	Понятие математической модели. Классификация математических моделей. Этапы математического моделирования. Принципы построения математических моделей. Основные математические структуры. Теория множеств и отношений. Математическая логика. Теория графов. Теория вероятностей. Математическая статистика. Аналитические методы. Численные методы. Статистические методы. Компьютерное моделирование. Имитационное моделирование.	ЛК, СЗ
Раздел 2	Модели безопасности компьютерных систем	2.1	Формальные модели безопасности	Модель Белла-ЛаПадулы. Модель Биба. Модель Clark-Wilson. Модель Brewer-Nash. Модель Graham-Denning. Дискреционное управление доступом. Мандатное управление доступом. Ролевое управление доступом. Управление доступом на основе атрибутов. Модель неинтерферирования. Модель безопасности на основе типов. Модели многоуровневых систем. Модели динамических систем.	ЛК, СЗ
Раздел 3	Методы анализа информационных потоков	3.1	Основы теории потоков информации	Определение информационных потоков. Классификация информационных потоков. Методы обнаружения потоков. Методы анализа потоков.	ЛК, СЗ
		3.2	Анализ конфиденциальности	Методы анализа утечек информации. Модели каналов утечки. Методы обнаружения аномалий. Метрики конфиденциальности.	ЛК, СЗ
		3.3	Анализ целостности	Методы контроля целостности. Модели нарушения целостности. Метрики целостности. Методы восстановления.	ЛК, СЗ
Раздел 4	Математические методы защиты информации	4.1	Криптографические методы	Симметричные криптосистемы. Асимметричные криптосистемы. Хеш-функции. Электронная подпись. Цифровая стеганография. Методы встраивания информации. Методы обнаружения. Оценка устойчивости.	ЛК, СЗ
		4.2	Методы аутентификации	Математические модели аутентификации. Протоколы аутентификации. Анализ надежности. Метрики безопасности.	ЛК, СЗ
		4.3	Методы обнаружения вторжений	Математические модели угроз. Статистические методы обнаружения. Машинное обучение в обнаружении вторжений. Оценка эффективности систем обнаружения.	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, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог. Мультимедийная доска.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 20 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	ОС Linux, Офисный пакет LibreOffice, ПО для просмотра формата pdf (например, evince), компилятор nasm, GNU Midnight Commander, Редактор emacs, Отладчики gdb и edb, Редактор vi, Компилятор gcc, Система управления версиями Git, Pandoc, Pandoc-crosref, TexLive, Julia
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.	ОС Linux, Офисный пакет LibreOffice, ПО для просмотра формата pdf (например, evince), компилятор nasm, GNU Midnight Commander, Редактор emacs, Отладчики gdb и edb, Редактор vi, Компилятор gcc, Система управления версиями Git, Pandoc, Pandoc-crosref, TexLive, Julia
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, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог. ОС Linux, Офисный пакет LibreOffice, ПО для просмотра формата pdf (например, evince), компилятор nasm, GNU Midnight Commander, Редактор emacs,

		Отладчики gdb и edb, Редактор vi, Компилятор gcc, Система управления версиями Git, Pandoc, Pandoc-crosref, TexLive, Julia
--	--	---

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

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Основная литература:

1. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст]: учебное пособие для вузов / П.Н. Девянин. — 3-е изд., перераб. и доп. — Москва: Горячая линия — Телеком, 2020. — 352 с.
2. Зариковская Н.В. Моделирование систем [Текст]: учебно-методическое пособие / Н.В. Зариковская. — Томск: ТУСУР, 2018. — 103 с. — ISBN 2227-8397.
3. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560426>

### Дополнительная литература:

1. Ибрагимов Н. Х. Практический курс дифференциальных уравнений и математического моделирования. Классические и новые методы. Нелинейные математические модели. Симметрия и принципы инвариантности / Н. Х. Ибрагимов; пер. с англ. И. С. Емельяновой. — 2-е изд., доп. и испр. — М.: Физматлит, 2012. — 332с.: ил. — Библиогр.: с. 322–325. — ISBN 978-5-9221-1377-9.
2. Трусов П. В. Введение в математическое моделирование / ред. П. В. Трусов; Ашихмин В. Н., Гитман М. Б., Келлер И. Э. и др. — М.: Логос, 2004. — 439 с. — ISBN 5-94010-272-7.
3. Andrews J. G., McLone R. R. Mathematical Modelling / Ed. by J. G. Andrews, R. R. McLone. — London: Butterworths, 1976. — 260 p. — ISBN 0408106018.
4. Боев, В. Д. Имитационное моделирование систем : учебник для вузов / В. Д. Боев. — Москва : Издательство Юрайт, 2025. — 253 с. — (Высшее образование). — ISBN 978-5-534-04734-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/563434>
5. Советов, Б. Я. Моделирование систем : учебник для вузов / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — Москва : Издательство Юрайт, 2025. — 343 с. — (Высшее образование). — ISBN 978-5-534-20145-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/557644>
6. Моделирование процессов и систем : учебник и практикум для вузов / Е. В. Стельмашонок, В. Л. Стельмашонок, Л. А. Еникеева, С. А. Соколовская ; под редакцией Е. В. Стельмашонок. — Москва : Издательство Юрайт, 2025. — 304 с. — (Высшее образование). — ISBN 978-5-534-18225-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560990>
7. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242>
8. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с.

— (Научная мысль). — DOI 10.12737/monography\_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2052391>

*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](http://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/>

- Научометрическая база данных Lens.org <https://www.lens.org>

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

1. Курс лекций по дисциплине «Методы математического моделирования в кибербезопасности».

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

**РАЗРАБОТЧИК:**

Профессор кафедры теории  
вероятностей и  
кибербезопасности

*Должность, БУП*

*Подпись*

Кулябов Дмитрий  
Сергеевич

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ БУП:**

Заведующий кафедрой теории  
вероятностей и  
кибербезопасности

*Должность БУП*

*Подпись*

Самуйлов Константин  
Евгеньевич

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ ОП ВО:**

Заведующий кафедрой теории  
вероятностей и  
кибербезопасности

*Должность, БУП*

*Подпись*

Самуйлов Константин  
Евгеньевич

*Фамилия И.О.*