

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 27.05.2026 12:33:09

Уникальный программный ключ:

ca953a01204891083f939673078ef1a989aae18a

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

ЭКОНОМИЧЕСКАЯ ОЦЕНКА УГРОЗ КИБЕРБЕЗОПАСНОСТИ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

38.03.05 БИЗНЕС-ИНФОРМАТИКА

(код и наименование направления подготовки/специальности)

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

КИБЕРБЕЗОПАСНОСТЬ В ЭКОНОМИКЕ

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Экономическая оценка угроз кибербезопасности» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 5 семестре 3 курса. Дисциплину реализует Кафедра экономико-математического моделирования. Дисциплина состоит из 5 разделов и 9 тем и направлена на изучение методов предиктивной аналитики, моделирования и формирования экспериментов для построения прикладных кейсов.

Целью освоения дисциплины является формирование и развитие у студентов навыков в области моделирования угроз и рисков кибербезопасности. Задачей курса является также обучение студентов использованию методов предиктивной аналитики, моделирования и формирования экспериментов для построения прикладных кейсов. Это позволит им при необходимости применять полученные знания и умения при решении практических задач в различных областях, связанных с предотвращением экономических угроз кибератак и киберпреступлений.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Экономическая оценка 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)
УК-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-10.1 Знает основные понятия социально-экономических наук и правила принятия решений в различных областях жизнедеятельности; УК-10.2 Умеет обосновывать и применять основные положения и методы социально-экономических наук для принятия решений в различных областях жизнедеятельности; УК-10.3 Владеет методами для принятия экономических решений в различных областях жизнедеятельности;
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1 Знает основные принципы самовоспитания и самообразования, исходя из требований рынка труда; УК-6.2 Умеет демонстрировать умение самоконтроля и рефлексии, позволяющие самостоятельно корректировать обучение по выбранной траектории; УК-6.3 Владеет способами управления своей познавательной деятельностью и удовлетворения образовательных интересов и потребностей;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	ПК-5.1 Знает методы организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.2 Знает основы нормативно-правового регулирования в РФ и иных странах в области защиты информации; ПК-5.3 Умеет применять методы управления кибербезопасностью предприятий и иных экономических систем; ПК-5.4 Умеет использовать нормативно-правовую базу РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем; ПК-5.5 Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.6 Владеет навыками применения нормативно-правовой

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		базы РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Экономическая оценка 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 «Экономическая оценка 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*
УК-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Микроэкономика; Макроэкономика; Экономика предприятия;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Рынки информационно-коммуникационных технологий и Индустрия 4.0; Мировая экономика; Финансовая безопасность; Seminar-Discussion on Business Informatics;
УК-6	Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	Введение в бизнес-информатику; <i>Психология и педагогика**</i> ; Технологии и практика программирования на языке Python для технических специальностей;	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем		Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Цифровая трансформация глобальной экономики; Анализ и показатели эффективности

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
			кибербезопасности предприятия; Искусственный интеллект и кибербезопасность; Кибербезопасность платежных систем; Технологии распределенного реестра Blockchain; Финансовая безопасность; Практикум по кибербезопасности предприятия. Часть 1; Практикум по кибербезопасности предприятия. Часть 2;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Экономическая оценка угроз кибербезопасности» составляет «3» 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)
			5
<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>	54		54
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	0		0
Общая трудоемкость дисциплины	ак.ч.	108	108
	зач.ед.	3	3

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	Имитационное моделирование как метод исследования	1.1	Основные понятия и области применения имитационного моделирования	Определение имитационного моделирования и его основные понятия. Классификация типов имитационных моделей. Области применения в экономике и кибербезопасности. Преимущества и ограничения метода имитационного моделирования.	ЛК, СЗ
		1.2	Стандарты, методики и инструменты, применяемые при аудите кибербезопасности	Международные и национальные стандарты аудита кибербезопасности. Основные методики проведения аудита экономических систем. Инструменты и программные средства для аудита кибербезопасности. Практические подходы к оценке рисков и уязвимостей.	ЛК, СЗ
Раздел 2	Моделирование экономических угроз в менеджменте	2.1	Процессное имитационное моделирование и его приложения в менеджменте и экономике	Понятие и принципы процессного имитационного моделирования. Построение и анализ бизнес-процессов с помощью имитации. Приложения в менеджменте и экономическом анализе. Примеры моделирования потоков и ресурсов в организациях.	ЛК, СЗ
		2.2	Модели и методы системной динамики: наиболее существенные приложения в менеджменте и экономике.	Основные модели системной динамики. Методы построения и анализа системно-динамических моделей. Приложения в стратегическом менеджменте и экономике. Примеры моделирования обратных связей и долгосрочных тенденций.	ЛК, СЗ
Раздел 3	Аудит кибербезопасности экономических систем	3.1	История развития искусственного интеллекта. Машинное обучение. Нейронные сети и их применение в предотвращении киберугроз.	История развития искусственного интеллекта. Основы машинного обучения и его виды. Архитектура и принципы работы нейронных сетей. Применение ИИ и нейросетей для выявления и предотвращения киберугроз.	ЛК, СЗ
		3.2	Многоагентное имитационное моделирование и поведенческая экономика	Понятие и структура многоагентных имитационных моделей. Моделирование взаимодействия агентов в экономических системах. Интеграция поведенческой экономики в имитационные модели. Применение для анализа коллективного поведения и рисков.	ЛК, СЗ
Раздел 4	Киберугроза и поведенческий анализ	4.1	Поведенческий анализ (на основе соц. графа и анализа вероятностей поведения потенциального киберпреступника)	Методы построения и анализа социальных графов. Вероятностный анализ поведения потенциального киберпреступника. Инструменты поведенческого профилирования в кибербезопасности. Применение для прогнозирования и предотвращения угроз.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		4.2	Инструменты экономического мошенничества в финансовой сфере	Основные виды и схемы экономического мошенничества. Инструменты и технологии, используемые в финансовом мошенничестве. Методы выявления и анализа мошеннических операций. Примеры реальных кейсов в банковской и финансовой сфере.	ЛК, СЗ
Раздел 5	Финансовое моделирование. Unit-экономика	5.1	«Электронное правительство»: когнитивные центры и аналитика стратегического планирования	Концепция электронного правительства и его компоненты. Роль когнитивных центров в государственном управлении. Аналитические инструменты стратегического планирования. Применение имитационного моделирования в государственных цифровых платформах.	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
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.	Microsoft Office, AnyLogic 8.9.6 или аналог
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

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Кузнецова, Е. И. Экономическая безопасность : учебник и практикум для вузов / Е. И. Кузнецова. — 2-е изд. — Москва : Издательство Юрайт, 2022. — 336 с. — (Высшее образование). — ISBN 978-5-534-14514-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490856>

2. Экономическая безопасность : учебник для вузов / Л. П. Гончаренко [и др.] ; под общей редакцией Л. П. Гончаренко. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 340 с. — (Высшее образование). — ISBN 978-5-534-06090-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/489082>

3. Мельников Сергей Юрьевич. Искусственный интеллект и кибербезопасность : учебное пособие / С.Ю. Мельников. - Электронные текстовые данные. - Москва : РУДН, 2023. - 72 с. : ил.

URL: https://lib.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=515838&idb=0

Дополнительная литература:

1. Уразгалиев, В. Ш. Экономическая безопасность : учебник и практикум для вузов / В. Ш. Уразгалиев. — Москва : Издательство Юрайт, 2018. — 374 с. — (Серия : Специалист). — ISBN 978-5-534-00484-7. — Текст: электронный // ЭБС Юрайт [сайт]. —

URL: <https://biblio-online.ru/bcode/4133482>

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

<http://lib.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 «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации

<http://docs.cntd.ru/>

- поисковая система Яндекс <https://www.yandex.ru/>

- поисковая система Google <https://www.google.ru/>

- реферативная база данных SCOPUS

<http://www.elsevierscience.ru/products/scopus/>

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

1. Курс лекций по дисциплине «Экономическая оценка угроз кибербезопасности».

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

РАЗРАБОТЧИК:

Старший преподаватель
кафедры экономико-
математического
моделирования

Должность, БУП

Подпись

Лазырин Михаил
Сергеевич

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
экономико-математического
моделирования

Должность БУП

Подпись

Балашова Светлана
Алексеевна

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории
вероятностей и
кибербезопасности

Должность, БУП

Подпись

Самуйлов Константин
Евгеньевич

Фамилия И.О.