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

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННЫМ ВОЗДЕЙСТВИЯМ В КИБЕРПРОСТРАНСТВЕ
(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)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Противодействие несанкционированным воздействиям в киберпространстве» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 5 семестре 3 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 6 разделов и 18 тем и направлена на изучение методов противодействия несанкционированным воздействиям в киберпространстве.

Целью освоения дисциплины является введение учащихся в предметную область современных методов, которые направлены на защиту частной, государственной, муниципальной и иных форм собственности в киберпространстве, защите объектов обеспечения кибербезопасности, защите интересов граждан и юридических лиц в информационной сфере, оказанию профессиональной помощи, консультированию по вопросам обеспечения кибербезопасности, осуществление экспертизы нормативных правовых актов, касающихся деятельности в области обеспечения кибербезопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Противодействие несанкционированным воздействиям в киберпространстве» 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-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 навыкками организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.6 Владеет навыками применения нормативно-правовой 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 «Противодействие несанкционированным воздействиям в киберпространстве» 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 «Противодействие несанкционированным воздействиям в киберпространстве».

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-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; Киберполитика в международных экономических отношениях; Искусственный интеллект в бизнесе; Дизайн мышление; Защита сетей и кибербезопасность; Анализ и показатели эффективности кибербезопасности предприятия; Искусственный интеллект и кибербезопасность; Киберполигон; Кибербезопасность платежных систем; Технологии распределенного реестра Blockchain;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Противодействие несанкционированным воздействиям в киберпространстве» 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
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.	*72*		*72*
Контроль (экзамен/зачет с оценкой), ак.ч.	*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	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Современная криминологическая оценка преступлений в сфере компьютерной информации.	1.1	Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации. Латентность преступлений в сфере компьютерной информации.	ЛК, СЗ
		1.2	Преступления, совершаемые с использованием глобальных компьютерных сетей.	ЛК, СЗ
		1.3	Понятие сетевого киберпреступления. Типология сетевых компьютерных преступлений.	ЛК, СЗ
Раздел 2	Уголовно-правовая характеристика киберпреступлений в сфере компьютерной информации по УК РФ.	2.1	Неправомерный доступ к компьютерной информации (ст. 272 УК). Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).	ЛК, СЗ
		2.2	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).	ЛК, СЗ
		2.3	Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК). Иные преступления, совершаемые с применением компьютерных технологий.	ЛК, СЗ
Раздел 3	Состояние и тенденции развития международного уголовного законодательства в сфере защиты компьютерной информации.	3.1	Правовые основы борьбы с преступлениями в киберпространстве в зарубежных странах. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.	ЛК, СЗ
		3.2	Общая характеристика и виды преступлений в киберпространстве по уголовному законодательству зарубежных стран. Сравнительно-правовой анализ отдельных преступлений в киберпространстве в зарубежном уголовном законодательстве. Международные соглашения в сфере борьбы с компьютерными преступлениями.	ЛК, СЗ
		3.3	Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ. Подходы различных государств к уголовно-правовому регулированию борьбы с преступлениями в глобальных компьютерных сетях.	ЛК, СЗ
Раздел 4	Причины и условия преступлений в киберпространстве.	4.1	Причины и условия преступлений в киберпространстве.	ЛК, СЗ
		4.2	Особенности личности преступника в сфере компьютерной информации. Типология личности преступника в сфере компьютерной информации.	ЛК, СЗ
		4.3	Особенности лиц, совершающих преступления в киберпространстве.	ЛК, СЗ
Раздел 5	Основные направления и меры борьбы с преступлениями в киберпространстве.	5.1	Основные направления профилактики преступлений в киберпространстве.	ЛК, СЗ
		5.2	Правовое регулирование борьбы с преступлениями в киберпространстве.	ЛК, СЗ
		5.3	Меры предупреждения преступлений в	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			киберпространстве.	
Раздел 6	Профилактика преступлений в киберпространстве.	6.1	Виктимологическая профилактика преступлений в киберпространстве.	ЛК, СЗ
		6.2	Система субъектов, осуществляющих борьбу с преступлениями в киберпространстве.	ЛК, СЗ
		6.3	Особенности предупреждения преступлений в глобальных компьютерных сетях.	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.	
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.	
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.	Персональный компьютер с доступом в интернет, Microsoft Teams

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Полякова Т. А., под редакцией, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844.

2. Ковалев Н. Н. Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2022. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496717.

3. Вехов В. Б. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — Москва : Издательство Юрайт, 2022. — 417 с. — (Высшее образование). — ISBN 978-5-534-14600-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497080.

Дополнительная литература:

1. Волков Ю. В. Информационное право. Информация как правовая категория : учебное пособие для вузов / Ю. В. Волков. — 2-е изд., стер. — Москва : Издательство Юрайт, 2022. — 109 с. — (Высшее образование). — ISBN 978-5-534-07052-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494255.

2. Шиханова Е. Г. Правовое регулирование инженерной деятельности : учебное пособие для вузов / Е. Г. Шиханова. — Москва : Издательство Юрайт, 2022. — 148 с. — (Высшее образование). — ISBN 978-5-534-13811-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496632.

3. Правовая информатика : учебник и практикум для вузов / под редакцией С. Г. Чубуковой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 314 с. — (Высшее образование). — ISBN 978-5-534-03900-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488822.

4. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/488767.

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»
- ЭБС «Лань» http://e.lanbook.com/
- ЭБС РГБ http://www.rsl.ru/

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/
- ресурсы Института научной информации по общественным наукам Российской академии наук (ИНИОН РАН) http://elibrary.ru
- университетская информационная система РОССИЯ. http://www.cir.ru/index.jsp
- Министерство экономического развития и торговли РФ http://economy.gov.ru
- Encyclopedia of Law and Economics http://allserv.rug.ac.be/~gdegeest
- библиотечка Либертариума – http://www.libertarium.ru/library
- Материалы по социально-экономическому положению и развитию в России – http://www.finansy.ru
- Мониторинг экономических показателей — http://www.budgetrf.ru

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

1. Курс лекций по дисциплине «Противодействие несанкционированным воздействиям в киберпространстве».
2. Практические задания по дисциплине «Противодействие несанкционированным воздействиям в киберпространстве»

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

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Противодействие несанкционированным воздействиям в киберпространстве» представлены в Приложении к настоящей Рабочей программе дисциплины.

* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.

РАЗРАБОТЧИК:

Доцент кафедры математического моделирования и искусственного интеллекта		Васильев Сергей Анатольевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

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