Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

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:

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)

2022 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Противодействие несанкционированным воздействиям в киберпространстве» 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): ПК-5

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	Способен решать задачи 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 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 части, формируемой участниками образовательных отношений, блока Б1 ОП ВО.

В рамках ОП ВО 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[1]
ПК-5	Способен решать задачи управления кибербезопасностью предприятий и иных экономических систем	Правовые основы кибербезопасности Цифровая трансформация глобальной экономики Международные платежные системы Дизайн мышление	Практическая защита сетей на основе анализа данных Анализ данных и показатели эффективности кибербезопасности предприятия Применение машинного обучения в кибербезопасности Преддипломная практика

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Противодействие несанкционированным воздействиям в киберпространстве» составляет 4 зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы		ВСЕГО, ак.ч.	Семестр(-ы)
			5
Контактная работа, ак.ч.		*36*	*36*
в том числе:			
Лекции (**ЛК**)		18	18
Лабораторные работы (**ЛР**)		-	-
Практические/семинарские занятия (**СЗ**)		18	18
Самостоятельная работа обучающихся, ак.ч.		*108*	*108*
Контроль (экзамен/зачет с оценкой), ак.ч.		-	-
Общая трудоемкость дисциплины	ак.ч.	**144**	**144**
	зач.ед.	**4**	**4**

[1]- заполняется в соответствии с матрицей компетенций и СУП ОП ВО

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы[2]
Раздел 1. Современная криминологическая оценка преступлений в сфере компьютерной информации.	Тема 1.1. Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации. Латентность преступлений в сфере компьютерной информации.	ЛР, СЗ
	Тема 1.2. Преступления, совершаемые с использованием глобальных компьютерных сетей.	ЛР, СЗ
	Тема 1.3. Понятие сетевого киберпреступления. Типология сетевых компьютерных преступлений.	ЛР, СЗ
Раздел 2. Уголовно-правовая характеристика киберпреступлений в сфере компьютерной информации по УК РФ	Тема 2.1. Неправомерный доступ к компьютерной информации (ст. 272 УК). Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).	ЛР, СЗ
	Тема 2.2. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК).	ЛР, СЗ
	Тема 2.3. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК). Иные преступления, совершаемые с применением компьютерных технологий.	ЛР, СЗ
Раздел 3. Состояние и тенденции развития международного уголовного законодательства в сфере защиты компьютерной информации	Тема 3.1. Правовые основы борьбы с преступлениями в киберпространстве в зарубежных странах. Подходы различных государств к криминализации преступлений в сфере компьютерной информации.	ЛР, СЗ
	Тема 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.	ЛР, СЗ
	Тема 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	ЛР, СЗ

[2]- заполняется только по ОЧНОЙ форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – семинарские занятия

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	преступлениями в глобальных компьютерных сетях.	
Раздел 4. Причины и условия преступлений в киберпространстве.	Тема 4.1. Причины и условия преступлений в киберпространстве.	ЛР, СЗ
	Тема 4.2. Особенности личности преступника в сфере компьютерной информации. Типология личности преступника в сфере компьютерной информации.	ЛР, СЗ
	Тема 4.3. Особенности лиц, совершающих преступления в киберпространстве.	ЛР, СЗ
Раздел 5. Основные направления и меры борьбы с преступлениями в киберпространстве.	Тема 5.1. Основные направления профилактики преступлений в киберпространстве.	ЛР, СЗ
	Тема 5.2. Правовое регулирование борьбы с преступлениями в киберпространстве.	ЛР, СЗ
	Тема 5.3. Меры предупреждения преступлений в киберпространстве.	ЛР, СЗ
Раздел 6. Профилактика преступлений в киберпространстве.	Тема 6.1. Виктимологическая профилактика преступлений в киберпространстве.	ЛР, СЗ
	Тема 6.2. Система субъектов, осуществляющих борьбу с преступлениями в киберпространстве.	ЛР, СЗ
	Тема 6.3. Особенности предупреждения преступлений в глобальных компьютерных сетях.	ЛР, СЗ

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. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций,	Компьютер/ноутбук с доступом сети Интернет и электронно-

	текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа презентаций.	образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
Для самостоятельной работы обучающихся	Аудитория 210 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. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

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 «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[3]:

1. Лабораторный практикум по дисциплине «Противодействие несанкционированным воздействиям в киберпространстве».

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

[3]- 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[4] оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Противодействие несанкционированным воздействиям в киберпространстве» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Доцент кафедры прикладной информатики и теории вероятностей		С.А. Васильев
Должность, БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Наименование БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Должность, БУП	Подпись	Фамилия И.О.

[4]- ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН