**Федеральное государственное автономное образовательное учреждение высшего образования**
**«Российский университет дружбы народов имени Патриса Лумумбы»**

**Факультет искусственного интеллекта**
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# МЕЖДУНАРОДНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ И КИБЕРТЕРРОРИЗМУ
(наименование дисциплины/модуля)

**Рекомендована МССН для направления подготовки/специальности:**

**10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**
(код и наименование направления подготовки/специальности)

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

**УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**
(наименование (профиль/специализация) ОП ВО)

**2026 г.**

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Международные аспекты противодействия киберпреступности и кибертерроризму» входит в программу магистратуры «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность» и изучается в 4 семестре 2 курса. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 1 раздела и 6 тем и направлена на изучение - основных международных и российских нормативных правовых актов и официальных документов по обеспечению информационной безопасности; - основных способов и методов противодействия преступности в сфере высоких технологий;

Целью освоения дисциплины является - сформировать единый подход к вопросам применения норм международного права при защите информации ограниченного доступа; - обеспечить углубленное изучение правовых и научных источников по данной тематике; - ознакомить с основными понятиями и методами противодействия киберпреступности; - рассмотреть наиболее проблемные вопросы теории и правоприменительной практики, касающиеся обеспечения информационной безопасности.ознакомить с основными понятиями и методами противодействия киберпреступности; - обеспечить теоретическую и практическую подготовку специалистов к деятельности, связанной с противодействием киберпреступности на локальном, национальном и международном уровнях.

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Международные аспекты противодействия киберпреступности и кибертерроризму» 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 | Способен формировать требования к защите информации в автоматизированных системах | ПК-3.1 Обосновывает необходимость защиты информации в автоматизированной системе;<br>ПК-3.2 Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой; |

## 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Международные аспекты противодействия киберпреступности и кибертерроризму» относится к части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Международные аспекты противодействия киберпреступности и кибертерроризму».

*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 | Способен формировать требования к защите информации в автоматизированных системах | *Инструментальные средства анализа рисков информационной безопасности***;<br>*Имитационное моделирование систем обеспечения информационной безопасности***;<br>*Системы обнаружения вторжений***;<br>*Методы выявления и анализа инцидентов информационной безопасности***; | |

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

** - элективные дисциплины /практики

## 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Международные аспекты противодействия киберпреступности и кибертерроризму» составляет «2» 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)** |
|---|---|---|---|
| | | | **4** |
| *Контактная работа, ак.ч.* | *32* | | *32* |
| Лекции (**ЛК**) | 16 | | 16 |
| Лабораторные работы (**ЛР**) | 0 | | 0 |
| Практические/семинарские занятия (**СЗ**) | 16 | | 16 |
| *Самостоятельная работа обучающихся, ак.ч.* | *22* | | *22* |
| *Контроль (экзамен/зачет с оценкой), ак.ч.* | *18* | | *18* |
| **Общая трудоемкость дисциплины** | **ак.ч.** | ***72*** | *72* |
| | **зач.ед.** | ***2*** | *2* |

## 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 | Международные аспекты противодействия киберпреступности и кибертерроризму | 1.1 | Информационно-телекоммуникационные технологии на современном этапе развития общества и их влияние на развитие международного сотрудничества | Социальные сети как инструмент цифровой дипломатии. Интернет вещей. НБИК-технологии и искусственный интеллект как стратегические вызовы для национальной и международной безопасности. Достижения информационно-коммуникационных технологий в арсенале средств массовой коммуникации. | ЛК, СЗ |
| | | 1.2 | Международное сотрудничество в ходе глобальной информационной революции в условиях ее влияния на политику и социум | Международные отношения под воздействием научно-технического прогресса. Новые реалии и проблемы международного права и этики цифровой экономики. Гражданское электронное общество и электронное государство. | ЛК, СЗ |
| | | 1.3 | Влияние угроз международной информационной безопасности на международное сотрудничество | Международная безопасность и государственный суверенитет в эпоху цифровых информационно-коммуникационных технологий. Практика информационного противоборства в контексте цифровых информационно-телекоммуникационных технологий. Информационно-телекоммуникационные технологии и информационные операции. Правонарушения в сфере обеспечения кибербезопасности. | ЛК, СЗ |
| | | 1.4 | Основы государственной политики Российской Федерации в области обеспечения международной информационной безопасности в работе ООН, ЮНЕСКО, БРИКС и СНГ и ее реализация | Деятельность ООН и ее специализированных учреждений в области международной информационной безопасности. Резолюции ГА ООН по защите критических информационных инфраструктур. Инициативы России в области международного сотрудничества по обеспечению информационной безопасности. Международный союз электросвязи и интернационализация управления Интернетом. ЮНЕСКО и МАГАТЕ в обеспечении международной информационной безопасности. Сотрудничество в области международной информационной безопасности в рамках ШОС. БРИКС как площадка международного сотрудничества в сфере информационной безопасности. Региональное взаимодействие в области международной информационной безопасности на пространстве СНГ и ОДКБ. | ЛК, СЗ |
| | | 1.5 | Реализация государственной политики Российской Федерации в области | «Группа двадцати» и ее роль в обеспечении международной информационной безопасности. ОБСЕ и Совет Европы в | ЛК, СЗ |

| Номер раздела | Наименование раздела дисциплины | Наименование темы | | Содержание темы | Вид учебной работы* |
|---|---|---|---|---|---|
| | | | международной информационной безопасности в работе ОБСЕ, Совета Европы и профильных площадок АТР | формировании мер доверия в сфере использования ИКТ. Профильные площадки АТР. Двусторонние межправительственные соглашения и межгосударственные договоренности в области международной информационной безопасности. | |
| | | 1.6 | Проблемные аспекты международного сотрудничества в ходе реализации альтернативных подходов США, ЕС и НАТО к обеспечению международной информационной безопасности | Эволюция подходов США к обеспечению международной информационной безопасности. Киберпространство НАТО как сфера военной деятельности. Базовые подходы ЕС к проблеме международной информационной безопасности. | 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. | Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. |
| 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. | Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска. |
| 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 или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет). |

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

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

*Основная литература:*

1. Международная информационная безопасность: теория и практика : в трех томах. Том 1 : учебник / под общ. ред А. В. Крутских. - 2-е изд., доп. - Москва : Издательство «Аспект Пресс», 2021. - 384 с. - ISBN 978-5-7567-1098-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1241985 (дата обращения: 16.04.2026). – Режим доступа: по подписке.

2. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В.С. Овчинский. — Москва : Норма : ИНФРА-М, 2024. — 528 с. - ISBN 978-5-91768-814-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2098567 (дата обращения: 16.04.2026)

3. Степанов, О. А. Противодействие кибертерроризму в цифровую эпоху : учебное пособие для вузов / О. А. Степанов. — Москва : Издательство Юрайт, 2026. — 103 с. — (Высшее образование). — ISBN 978-5-534-19963-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588068 (дата обращения: 16.04.2026).

*Дополнительная литература:*

1. Гасумянов, В. И. Информационная безопасность : международный аспект : учебное пособие / В. И. Гасумянов, Д. И. Григорьев ; Московский государственный институт международных отношений (университет) МИД России, Международный институт энергетической политики и дипломатии, Базовая кафедра ПАО «ГМК “Норильский никель”». – Москва : МГИМО-Университет, 2024. – 226 с. : табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=730591 (дата обращения: 16.04.2026). – Библиогр.: с. 219-222. – ISBN 978-5-9228-2856-7. – Текст : электронный.

2. Бирюков Алексей Викторович, Алборова Марианна Борисовна. Социально-гуманитарные риски информационного общества и международная информационная безопасность. монография [Электронный ресурс]. - М. : Аспект Пресс, 2021. 95 с. ISBN 978-5-7567-1126-4 URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=505684&idb=0 (дата обращения: 16.04.2026)

3. Зинченко Александр Викторович. Архитектоника международной информационной безопасности. монография [Электронный ресурс]. - М. : Аспект Пресс, 2021. 159 с. ISBN 978-5-7567-1131-8 URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=500270&idb=0 (дата обращения: 16.04.2026)

4. Красинский Владислав Вячеславович. Терроризм 2.0. монография [Электронный ресурс]. - М. : Юрлитинформ, 2023. 262 с. ISBN 978-5-4396-2438-6 URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=509242&idb=0 (дата обращения: 16.04.2026)

*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 «Международные аспекты противодействия киберпреступности и кибертерроризму».

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

**РАЗРАБОТЧИК:**

| Заведующий кафедрой информационной безопасности | | Царегородцев Анатолий Валерьевич |
|---|---|---|
| *Должность, БУП* | *Подпись* | *Фамилия И.О.* |

**РУКОВОДИТЕЛЬ БУП:**

| Заведующий кафедрой информационной безопасности | | Царегородцев Анатолий Валерьевич |
|---|---|---|
| *Должность БУП* | *Подпись* | *Фамилия И.О.* |

**РУКОВОДИТЕЛЬ ОП ВО:**

| Заведующий кафедрой информационной безопасности | | Царегородцев Анатолий Валерьевич |
|---|---|---|
| *Должность, БУП* | *Подпись* | *Фамилия И.О.* |