Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 06.06.2025 11:43:04

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a989dae18a

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)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «International Legal Frameworks for Combating Cybercrime and Cyberterrorism» входит в программу магистратуры «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность» и изучается в 4 семестре 2 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 6 разделов 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; 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	<i>Инструментальные средства анализа рисков информационной безопасности**;</i> <i>Имитационное моделирование систем обеспечения информационной безопасности**;</i> <i>Системы обнаружения вторжений**;</i> <i>Методы выявления и анализа инцидентов информационной безопасности**;</i>	

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «International Legal Frameworks for Combating Cybercrime and Cyberterrorism» 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
<i>Контактная работа, ак.ч.</i>	32		32
Лекции (ЛК)	16		16
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	16		16
<i>Самостоятельная работа обучающихся, ак.ч.</i>	31		31
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	9		9
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	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Информационно-телекоммуникационные технологии на современном этапе развития общества и их влияние на развитие международного сотрудничества	1.1	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
Раздел 2	Международное сотрудничество в ходе глобальной информационной революции в условиях ее влияния на политику и социум	2.1	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
Раздел 3	Влияние угроз международной информационной безопасности на международное сотрудничество	3.1	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
Раздел 4	Основы государственной политики Российской Федерации в области обеспечения международной информационной безопасности в работе ООН, ЮНЕСКО, БРИКС и СНГ и ее реализация	4.1	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
Раздел 5	Реализация государственной политики Российской Федерации в области международной информационной безопасности в работе ОБСЕ, Совета Европы и профильных площадок АТР	5.1	«Группа двадцати» и ее роль в обеспечении международной информационной безопасности. ОБСЕ и Совет Европы в формировании мер доверия в сфере использования ИКТ. Профильные площадки АТР. Двусторонние межправительственные соглашения и межгосударственные договоренности в области международной информационной безопасности.	ЛК, СЗ
Раздел 6	Проблемные аспекты международного	6.1	Эволюция подходов США к обеспечению международной информационной безопасности.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
	сотрудничества в ходе реализации альтернативных подходов США, ЕС и НАТО к обеспечению международной информационной безопасности		Киберпространство НАТО как сфера военной деятельности. Базовые подходы ЕС к проблеме международной информационной безопасности.	

* - 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.	

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Окинавская хартия глобального информационного общества. 22 июля 2000 г.
2. «Стратегия национальной безопасности Российской Федерации до 2020 г.»
Указ Президента РФ №537 от 12.05.2009
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ в декабре 2016 г. № Пр-1895).
4. «О подписании Соглашения о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности». Расп. Пр. РФ от 28.05.2012 № 856-р

«Собрание законодательства РФ», 04.06.2012, № 23, ст. 3058.

5. Международная информационная безопасность: Теория и практика: В 3-х т. Учебник для вузов МГИМО/Под общ. ред. А.В. Крутских. – М.: «Аспект-пресс». 2019. – 384 с.

Дополнительная литература:

1. Стрельцов А.А. Информационная безопасность Российской Федерации. – М.: Высшая школа, 2003.

2. Копылов В.А. Информационное право. – М., 2011. – М.: Юридические науки. – 247 с.

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/>

- 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 «Международные аспекты противодействия кибертерроризму».

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

РАЗРАБОТЧИК:

<hr/> <i>Должность, БУП</i>	<hr/> <i>Подпись</i>	<hr/> Баум Валентина Владимировна <i>Фамилия И.О.</i>
-----------------------------	----------------------	---

РУКОВОДИТЕЛЬ БУП:

<hr/> Заведующий кафедрой <i>Должность БУП</i>	<hr/> <i>Подпись</i>	<hr/> Подолько Павел Михайлович [М] заведующий кафедрой <i>Фамилия И.О.</i>
---	----------------------	--

РУКОВОДИТЕЛЬ ОП ВО:

<hr/> <i>Должность, БУП</i>	<hr/> <i>Подпись</i>	<hr/> <i>Фамилия И.О.</i>
-----------------------------	----------------------	---------------------------