Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 27.02.2025 15:51:11
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 / INTERNATIONAL LEGAL FRAMEWORKS FOR COMBATING CYBERCRIME AND CYBERTERRORISM

(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 «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 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	*Инструментальные средства анализа рисков информационной безопасности***; *Имитационное моделирование систем обеспечения информационной безопасности***; *Системы обнаружения вторжений***; *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.	*31*		*31*
Контроль (экзамен/зачет с оценкой), ак.ч.	*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

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 6	Проблемные аспекты международного сотрудничества в ходе реализации альтернативных подходов США, ЕС и НАТО к обеспечению международной информационной безопасности	6.1	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	Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand _25, двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Семинарская	Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand _25, двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной	Компьютерный класс для проведения лабораторно-практических занятий, курсового проектирования, практической подготовки. Комплект специализированной мебели; доска маркерная; технические средства: персональные компьютеры, проекционный экран, мультимедийный проектор, NEC NP-V302XG, выход в Интернет. Программное обеспечение: продукты Microsoft (ОС,

	мебели и компьютерами с доступом в ЭИОС.	пакет офисных приложений, в т.ч. MS Office/Office 365, Teams, Skype), Autodesk AutoCAD 2021, Autodesk AutoCAD 2021 (англ. яз.), Autodesk Inventor 2021, Autodesk Revit 2021, ArchiCAD 23 (бесплатные учебные версии)
		Компьютерный класс - учебная аудитория для практической подготовки, лабораторно-практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также самостоятельной работы Комплект специализированной мебели; (в т.ч. электронная доска); мультимедийный проектор BenqMP610; экран моторизованный Sharp 228*300; доска аудиторная поворотная; Комплект ПК iRU Corp 317 TWR i7 10700/16GB/ SSD240GB/2TB 7.2K/ GTX1660S-6GB /WIN10PRO64/ BLACK + Комплект Logitech Desktop MK120, (Keybord&mouse), USB, [920-002561] + Монитор HP P27h G4 (7VH95AA#ABB) (УФ-000000000059453)-5шт., Компьютер Pirit Doctrin4шт., ПО для ЭВМ LiraServis Academic Set 2021 Состав пакета ACADEMIC SET: программный комплекс "ЛИРА-САПР FULL". программный комплекс "МОНОМАХ-САПР PRO". программный комплекс "ЭСПРИ.

* - 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 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 «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**!

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 «Международные аспекты противодействия киберпреступности и кибертерроризму» представлены в Приложении к настоящей Рабочей программе дисциплины.

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