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

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

(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 «Информационно-психологическая безопасность» 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 5 разделов и 5 тем и направлена на изучение сновных условий и факторов нарушения индивидуальной психологической безопасности; изучить современных моделей достижения личностью информационно-психологической безопасности в современном социуме.

Целью освоения дисциплины является приобретение обучающимися теоретических знаний и практических навы-ков по эффективному построению отношений с лицами, оказывающими влияние на информационную безопасность организации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Информационно-психологическая безопасность» 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)
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1 Находит и использует при социальном и профессиональном общении информацию о культурных особенностях и традициях различных социальных групп; УК-5.2 Обосновывает особенности проектной и командной деятельности с представителями других этносов и (или) конфессий;
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.1 Анализирует свои ресурсы и их пределы (личностные, ситуативные, временные и т.д.), для успешного выполнения поставленной задачи;
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Обосновывает требования к системе обеспечения информационной безопасности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Информационно-психологическая безопасность» относится к обязательной части 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 «Информационно-психологическая безопасность».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Профессиональное общение и межкультурное взаимодействие в команде;	
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Научно-исследовательская работа; Управление проектами; Управление информационной безопасностью;	
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Теория игр и исследование операций; Защищенные информационные системы; Технологии обеспечения информационной безопасности; Управление информационной безопасностью; Разработка технической документации;	

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Информационно-психологическая безопасность» 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)**
			4
Контактная работа, ак.ч.	*48*		*48*
Лекции (**ЛК**)	24		24
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	24		24
Самостоятельная работа обучающихся, ак.ч.	*42*		*42*
Контроль (экзамен/зачет с оценкой), ак.ч.	*18*		*18*
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	Тема 1. Концептуальные основы информационно-психологической безопасности личности, общества, государства.	1.1	Сущность понятий «опасность» и «безопасность». Основные информационные угрозы и национальные интересы России в информационной сфере. Основы универсальной взаимосвязи видов, объектов и средств борьбы. Топология объекта информационно-психологического воздействия. Универсальные признаки информационных характеристик объектов. Критически важные аспекты информационно-психологической безопасности. Сущность информационно-психологического воздействия. Сущность защиты от информационно-психологического воздействия.	ЛК, СЗ
Раздел 2	Информационное воздействие и защита от него.	2.1	Содержание и средства информационно-психологического воздействия. Основания методологии анализа аспектов воздействий на общественное сознание. Уровни психической деятельности как среда для воздействий. Мишени информационно-психологического воздействия на социальные объекты. Направления программирования общественного сознания. Место смысловых аспектов в модельном мире субъекта. Актуальные направления и темы разрушения общественного сознания. Приемы информационно-психологического воздействия. Виды информационно-психологической защиты личности. Алгоритм информационно-психологической самозащиты.	ЛК, СЗ
Раздел 3	Морально-этические аспекты информационно-психологической безопасности.	3.1	Культурные и этические основания развития цивилизации. Этические воззрения и виды этики. Мораль как предмет этики и условие информационно-психологической безопасности. Функции морали и этические категории, обусловливающие формирование информационно-психологической безопасности. Основные свойства коммуникации посредством интернета и угрозы информационной безопасности вследствие неэтичного поведения в сети. Основные этические принципы и нормы взаимодействия в интернете в интересах обеспечения информационно-психологической безопасности.	ЛК, СЗ
Раздел 4	Этические аспекты обеспечения информационной безопасности профессионалами.	4.1	Основы профессиональной этики в области ИТ. Профессиональные отношения. Функции профессионального кодекса этики. Обязательства ИТ-профессионалов перед обществом, работодателем, заказчиками, коллегами. Кодексы этики в области обеспечения безопасности информационных систем. Принципы кодексов этики ACM/IEEE-CS, Единого кодекса этики профессионального поведения.	ЛК, СЗ
Раздел 5	Средства массовой информации и реклама как каналы	5.1	Коммуникативные функции рекламы. Технологии воздействия через СМИ и рекламную деятельность. Угрозы	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
	информационно-психологического воздействия.		манипулирования в рекламе. Формирование доверия к коммуникатору. Принципы подачи рекламных материалов и подготовки сообщений в СМИ. Роль органов управления и пресс-служб в недопущении деструктивных информационных воздействий через СМИ и рекламно-выставочную деятельность. Основы защиты информации в выставочной и публикаторской деятельности.	

* - 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. Грачев Г.В., Мельник И.К. Манипулирование личностью: организация, способы и технологии информационного воздействия. Из-во Алгорим, 2002.

2. Зелинский С.А. Манипулирование Личностьюи массами. Манипулятивные технологии власти при атаке на подсознание индивида и масс. – Спб.:Издательско-Торговый дом «СКИФИЯ», 2008. – 240.

3. Международная инфомационная безопасность: Теория и практика: В трех томах.

Учебник для вузов / Под общ. Ред. А.В. Крутских. – М.: Издательство Аспект Пресс», 2019.

4. Международое право: Учебник для бакалавров / Отв. Ред. Р.М. Валеев, Г.И. Курдюков. – М.: Статут, 2017.

5. Федеральный закон № 5485-1 «О государственной тайне», 21 июля 1993 г. (с изм. от 6.10.97 г. и от 11.12.2011 г.). – М.: МВК по ЗГТ, 2011.

6. «Стратегия национальной безопасности Российской Федерации до 2020 г.». Указ Президента РФ №537 от 12.05.2009

Дополнительная литература:

1. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

2. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

3. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 2003.

4. Журавлев С.Ю. «Частная охрана». – М.: 1994.

5. Окинавская хартия глобального информационного общества. 22 июля 2000 г.

6. Гражданский кодекс Российской Федерации. Часть IV.

7. Федеральный закон № 310-ФЗ «О безопасности», 26 декабря 2010 г.

8. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).

9. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07. 2006 г. № 149-ФЗ.

10. «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.

11. Постановление правительства РФ «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в ФОИВ» № 1233 от 03 ноября 1994 г. – М.: МВК по ЗГТ, 1998.

12. Постановление правительства РФ «Об утверждении правил отнесения сведений к различным степеням секретности» № 170 от 20 февраля 1995 г. – М.: МВК по ЗГТ, 1998.

13. Инструкция о порядке допуска должностных лиц и граждан РФ к государственной тайне. Постановление Правительства РФ от 6 февраля 2010 г. № 63

14. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.

15. «Об утверждении Типовой инструкции по делопроизводству в ФОИВ»: Пр. Федеральной архивной службы России от 27.11.2000 г. № 68.

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

17. Рассолов И.М. Информационное право. Учебник. – М.: Норма: ИНФРА-М, 2010. – 352 с.

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

19. Садердинов А.А. Информационная безопасность предприятия. Уч. пособие. – М.: Дашков и Ко, 2004.

20. Федеральный закон № 98-ФЗ «О коммерческой тайне», 29 июля 2004 г.

21. Федеральный закон № 152-ФЗ «О персональных данных», 27 июля 2006 г.

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 «Информационно-психологическая безопасность».

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

РАЗРАБОТЧИК:

		Баум Валентина Владимировна
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

		Подолько Павел Михайлович [М|]
Заведующий кафедрой		заведующий кафедрой
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

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