

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 22.05.2026 10:55:39

Уникальный программный ключ:

sa953a01204891083f939673078ef1a989dae18a

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

ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/специальности)

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

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Гуманитарные аспекты информационной безопасности» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра информационной безопасности. Дисциплина состоит из 1 раздела и 8 тем и направлена на изучение освоение гуманитарной сущности информационной безопасности, концепций информационного противоборства, методов и технологий информационно-психологического воздействия на групповое и массовое сознание, а также способов защиты информационного пространства и обеспечения информационного суверенитета.

Целью освоения дисциплины является формирование у обучающихся системы знаний о гуманитарных аспектах информационной безопасности, парадигмах безопасности, теории информационного противоборства, классификации информационно-психологического оружия, лексических, грамматических и невербальных способах воздействия на общественное сознание, а также умений и практических навыков выявления, анализа и нейтрализации манипулятивных технологий и информационно-психологических угроз в профессиональной деятельности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Гуманитарные аспекты информационной безопасности» 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-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1 Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели; УК-3.2 Формулирует и учитывает в своей деятельности особенности поведения групп людей, выделенных в зависимости от поставленной цели;
ПК-4	Способен разрабатывать комплекс организационных мер по защите информации на объекте информатизации	ПК-4.2 Организует работы по внедрению организационных мер для выполнения требований защиты информации ограниченного доступа в автоматизированных системах;
ПК-5	Способен организовывать и проводить общепрофилактические, адресные, индивидуальные мероприятия по противодействию распространения идеологии терроризма и идей неонацизма	ПК-5.1 Определяет содержание и формы профилактической работы по противодействию идеологии терроризма и неонацизма в соответствии с действующими нормативными правовыми актами; ПК-5.2 Организует и проводит профилактические мероприятия в образовательной или социальной среде в соответствии с установленными требованиями и нормативными документами;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Гуманитарные аспекты информационной безопасности» 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 «Гуманитарные аспекты информационной безопасности».

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-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	Ознакомительная практика; Исследовательская практика; Основы управленческой деятельности;	Преддипломная практика; Технологическая практика;
ПК-4	Способен разрабатывать комплекс организационных мер по защите информации на объекте информатизации	<i>Information Security International Standards**;</i> <i>International Issues of Internet Governance**;</i> <i>Теория систем и системный анализ**;</i> <i>Методы принятия решений**;</i>	<i>Организация и управление службой защиты информации**;</i> <i>Информационно-аналитическая деятельность по обеспечению комплексной безопасности**;</i> Преддипломная практика;
ПК-5	Способен организовывать и проводить общепрофилактические, адресные, индивидуальные мероприятия по противодействию распространения идеологии терроризма и идей неонацизма	<i>Основы военной подготовки. Безопасность жизнедеятельности;</i>	Преддипломная практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Гуманитарные аспекты информационной безопасности» 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)
			6
<i>Контактная работа, ак.ч.</i>	52		52
Лекции (ЛК)	26		26
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	26		26
<i>Самостоятельная работа обучающихся, ак.ч.</i>	38		38
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	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	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Гуманитарные аспекты информационной безопасности	1.1	Гуманитарная сущность безопасности	Понятия «безопасность» и «гуманитарный». Концепции сущности информации. Гуманитарная сущность информации. Аспекты гуманитарной сущности информационной безопасности. Цель обеспечения информационной безопасности. Социально-гуманитарная сущность понятия безопасности, зафиксированная в нормативно-правовых актах России по вопросам безопасности. Парадигмы безопасности: парадигма защищенности и парадигма развития. Гуманитарные технологии информационно-психологического воздействия на групповое и массовое сознание. Проблема защиты информационного пространства от внешнего негативного влияния современных информационно-телекоммуникационных технологий для дестабилизации внутривнутриполитической и социальной ситуации.	ЛК, СЗ
		1.2	Теория информационного противоборства: основные понятия.	Основные термины и определения. Информационное противоборство как форма борьбы сторон для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах. Сферы информационного противоборства. Основные доктрины манипуляции массовым сознанием. Геополитическое информационное противоборство. Уровни ведения информационного противоборства. Принципы, задачи, методы информационного противоборства. Объекты воздействия. Информационно-техническое и информационно-психологическое противоборство. Составные части информационного противоборства. Алгоритмы выработки решений в ходе информационного противоборства.	ЛК, СЗ
		1.3	Информационно-коммуникационные технологии воздействия на групповое и массовое сознание	Суть коммуникативных процессов и место человека в них. Анализ концепций информационно-психологических аспектов массовой коммуникации. Защита от информации. Информационный суверенитет. Электронный (цифровой) суверенитет. Информационно-психологическое воздействие на человека и манипуляция групповым и массовым сознанием. Основные структурные элементы информационно-	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				психологического воздействия: дезинформация, лоббирование, манипулирование, пропаганда, управление кризисами, шантаж.	
		1.4	Информационно-психологическое оружие	Возможности человека по восприятию информации и форм ее представления. Модели обработки информации органами зрения, слуха, обоняния и вкуса. Воздействие информации через информационно-коммуникационные средства на память человека. Классификация информационно-психологического оружия. Определение понятия информационно-психологического оружия. Объекты воздействия информационно-психологического оружия. Информативные каналы передачи признаков состояния человека. Оружие средств массовой информации. Энергоинформационное психологическое оружие. Психотронно-информационное оружие. Биоэнергетическое оружие. Методы лингвистической борьбы.	ЛК, СЗ
		1.5	Вербальные способы реализации латентного воздействия на групповое и массовое сознание	Язык слов. Магическая сила слова. Правильный и туземный языки. Политический язык. Воздействие на ткань языка в идеологических целях. Язык образов. Язык чисел и меры. Воздействие на различные виды памяти. Воздействие на историческую память. Воздействие на логическое и рациональное мышление. Воздействие на аутистическое сознание. Воздействие на ассоциативное мышление. Метафоры и стереотипы.	ЛК, СЗ
		1.6	Лексические и грамматические способы воздействия на общественное сознание	Лексико-семантические варианты. Использование эвфемизмов и дисфемизмов. Приемы использования ассоциативного поля. Использование в исторических параллелях имен собственных. Использование категории одушевленности. Использование приемов введения экспертов, универсальной истины, модальности и интерпретации скрытых смыслов. Использование синтаксических способов: повтора, построения параллельных конструкций, градации. Использование приемов формальной логики: подмена аргумента, перенос смыслового акцента.	ЛК, СЗ
		1.7	Использование вербальных и невербальных способов воздействия на групповое и массовое сознание	Использование ольфакторной сферы для манипуляции индивидуальным, групповым и массовым сознанием. Экстралингвистические способы на сознание и подсознание.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				<p>Звуковое воздействие в процессе социальной регуляции. Манипулятивные технологии. Параметры технологий: частота использование приёмов, широта и разнообразие применения, степень действительности. Реклама как форма проявления вербального и невербального манипулирования. Систематизация приёмов информационно-психологического воздействия. Манипулятивный эффект.</p>	
		1.8	Оружие средств массовой информации	<p>Использование устного вещания, печатных и изобразительных средств, радио и телевидения, аудио-видео- и киносредств для манипулятивного воздействия на групповое и массовое сознание. СМИ и общественное мнение. Формирование общественного мнения как средство достижения успеха в мировой политике. Композиция информации в прессе. Организация подачи информации в рамках номера печатного издания. Система ценностей общества как объект воздействия СМИ. Социолингвистический анализ используемых форм политического насилия средствами массовой информации в изменении поведения гражданского общества.</p>	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. Дербин, Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности : учебное пособие / Е.А. Дербин, А.В. Царегородцев. — Москва : ИНФРА-М, 2024. — 267 с. — (Высшее образование). — DOI 10.12737/2084342. - ISBN 978-5-16-019050-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2084342> (дата обращения: 09.04.2026). – Режим доступа: по подписке.

2. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебник для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2026. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589310> (дата обращения: 09.04.2026).

Дополнительная литература:

1. Рабчевский, А. Н. Основы информационного противоборства: сетевая наука : учебник для вузов / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2026. — 202 с. —

(Высшее образование). — ISBN 978-5-534-19085-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589700> (дата обращения: 09.04.2026).

2. Бартош, А. А. Основы международной безопасности. Организации обеспечения международной безопасности : учебник для вузов / А. А. Бартош. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 429 с. — (Высшее образование). — ISBN 978-5-534-17521-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/586154> (дата обращения: 09.04.2026).

3. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие : [16+] / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; под науч. ред. А. Г. Волеводза ; Московский государственный институт международных отношений (университет) МИД России. — Москва : Прометей, 2023. — 1086 с. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=701090> (дата обращения: 09.04.2026). — Библиогр. в кн. — ISBN 978-5-00172-447-6. — Текст : электронный.

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 «Гуманитарные аспекты информационной безопасности».

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

РАЗРАБОТЧИК:

Заведующий кафедрой
информационной безопасности

Должность, БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
информационной безопасности

Должность БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой
информационной безопасности

Должность, БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.