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

Высшая школа управления
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

38.03.02 МЕНЕДЖМЕНТ
(код и наименование направления подготовки/специальности)

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

ЦИФРОВОЙ ДИЗАЙН И ВЕБ-РАЗРАБОТКА
(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы кибербезопасности» входит в программу бакалавриата «Цифровой дизайн и веб-разработка» по направлению 38.03.02 «Менеджмент» и изучается в 4 семестре 2 курса. Дисциплину реализует Кафедра математического моделирования и информационных технологий. Дисциплина состоит из 4 разделов и 12 тем и направлена на изучение основных понятий и принципов кибербезопасности, технических и организационных мер защиты методов реагирования на инциденты и восстановления после кибератак, включая планирование непрерывности бизнеса, применения искусственного интеллекта для обнаружения угроз, автоматизации защиты и прогнозирования киберрисков.

Целью освоения дисциплины является формирование у обучающихся системные знания, практические навыки и компетенции, необходимые для защиты информации, цифровых платформ и бизнес-процессов от современных киберугроз, а также для эффективного реагирования на инциденты и обеспечения непрерывности деятельности в условиях цифровизации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы кибербезопасности» 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-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	УК-12.1 Осуществляет поиск нужных источников информации и данных, воспринимает, анализирует, запоминает и передает информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; УК-12.2 Проводит оценку информации, ее достоверность, строит логические умозаключения на основании поступающих информации и данных;
ПК-1	Способность осуществлять тактическое планирование деятельности структурных подразделений производственной организации	ПК-1.1 Владеет методами анализа конкретных условий и потребностей рынка;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы кибербезопасности» 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 «Основы кибербезопасности».

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-12	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	Цифровая грамотность; Деловые коммуникации; Статистика; *Информатика***; *Цифровая экономика***; *Компьютерный практикум по информационным технологиям***; *Продвинутый Excel***; *Прикладной анализ данных с использованием языка Python***; *3D-моделирование и основы анимации***; Информационные и цифровые технологии в управлении предприятием;	Производственно-управленческая практика; Преддипломная практика; Основы PHP; Эконометрика; Базы данных, алгоритмы и структуры данных; *Управление продуктом***; *Электронный бизнес***; *Startup и привлечение инвестиций***; Прикладной искусственный интеллект в менеджменте; *ИИ в дизайне***; *Визуальные коммуникации***; *Нейросети в дизайне***; UX; Основы программирования на Java; Автоматизация бизнес-процессов; Аналитика данных (BI); Компьютерная графика; SQL-программирование;
ПК-1	Способность осуществлять тактическое планирование деятельности структурных подразделений производственной организации	Основы веб-дизайна; Основы дизайна; Основы веб-разработки; Ознакомительная практика;	Эконометрика; Дизайн мобильных приложений; Основы геймдизайна; *Управление разработкой программного обеспечения***; *Управление цифровой трансформацией***; *Архитектура программного обеспечения***; *Рынки ИКТ и организация продаж***; *Технологии искусственного интеллекта***; *Личный бренд и лидерство***; Преддипломная практика; Производственно-управленческая практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы кибербезопасности» 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.	*34*		*34*
Лекции (**ЛК**)	17		17
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	17		17
Самостоятельная работа обучающихся, ак.ч.	*20*		*20*
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	Основы информационной безопасности	1.1	Конфиденциальность, целостность, доступность	Ключевые принципы защиты информации, их значение и реализация в современных системах.	ЛК, СЗ
		1.2	Угрозы и уязвимости	Классификация основных угроз (вирусы, фишинг, DDoS-атаки), анализ уязвимостей программного и аппаратного обеспечения.	ЛК, СЗ
		1.3	Политики и стандарты безопасности	Разработка и внедрение корпоративных политик, соответствие международным и национальным стандартам.	ЛК, СЗ
Раздел 2	Технические средства защиты	2.1	Антивирусная защита и межсетевые экраны	Принципы работы, настройка и обновление средств защиты от вредоносного ПО и несанкционированного доступа.	ЛК, СЗ
		2.2	Шифрование данных и управление доступом	Методы криптографической защиты, системы идентификации и аутентификации пользователей.	ЛК, СЗ
		2.3	Резервное копирование и восстановление	Организация процессов резервирования, стратегии восстановления после сбоев и атак.	ЛК, СЗ
Раздел 3	Организационные и правовые аспекты	3.1	Человеческий фактор и социальная инженерия	Обучение сотрудников, профилактика фишинга, повышение киберграмотности.	ЛК, СЗ
		3.2	Правовое регулирование и ответственность	Законодательство в сфере кибербезопасности, ответственность за нарушения, порядок расследования инцидентов.	ЛК, СЗ
		3.3	Управление инцидентами и непрерывность бизнеса	Алгоритмы реагирования на инциденты, разработка планов обеспечения непрерывности деятельности.	ЛК, СЗ
Раздел 4	Искусственный интеллект в кибербезопасности	4.1	AI для обнаружения аномалий и угроз	Применение машинного обучения для анализа сетевого трафика, выявления подозрительной активности и новых типов атак.	ЛК, СЗ
		4.2	Автоматизация реагирования на инциденты	Интеллектуальные системы для автоматического блокирования угроз, минимизации ущерба и ускорения восстановления.	ЛК, СЗ
		4.3	Прогнозирование киберрисков и моделирование атак	Использование AI для оценки вероятности угроз, тестирования защищённости и подготовки к новым сценариям атак.	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.	
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. Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2026. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/589431 (дата обращения: 17.04.2026).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374 (дата обращения: 17.04.2026).

Дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741 (дата обращения: 17.04.2026).

2. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590420 (дата обращения: 17.04.2026).

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 «Основы кибербезопасности».

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

РАЗРАБОТЧИК:

Старший преподаватель		Роэков Андей Павлович
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Кокуйцева Татьяна Владимировна [М|] заведующий каф
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой		Кокуйцева Татьяна Владимировна [М|] заведующий каф
Должность, БУП	*Подпись*	*Фамилия И.О.*