**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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(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 информационной безопасности» 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 3 разделов и 11 тем и направлена на изучение основ защиты информации и управление рисками в сфере информационной безопасности организаций.

Целью освоения дисциплины является формирование у студентов знаний об информационной безопасности, роль и значении обеспечения информационной безопасности в профессиональной деятельности.Задачи дисциплины: • получение знаний о современных информационных системах, нормативно-правовых документах РФ, методах и средствах обеспечения информационной безопасности;• умений выявлять возможные угрозы, влияющие на состояние информационной безопасности;• организовывать мероприятия по выполнению требований нормативных и руководящих документов РФ, проведении политики безопасности предприятия в области обеспечения информационной безопасности;• владеть практическими навыками по использованию современных методов и средств обеспечения информационной безопасности

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы 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-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;<br>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 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 «Основы 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-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;<br>Деловые коммуникации;<br>Статистика;<br>*Информатика***;<br>*Цифровая экономика***;<br>*Компьютерный практикум по информационным технологиям***;<br>*Продвинутый Excel***;<br>*Прикладной анализ данных с использованием языка Python***;<br>*3D-моделирование и основы анимации***;<br>Информационные и цифровые технологии в управлении предприятием; | Производственно-управленческая практика;<br>Преддипломная практика;<br>Основы PHP;<br>Эконометрика;<br>Базы данных, алгоритмы и структуры данных;<br>*Управление продуктом***;<br>*Электронный бизнес***;<br>*Startup и привлечение инвестиций***;<br>Прикладной искусственный интеллект в менеджменте;<br>*ИИ в дизайне***;<br>*Визуальные коммуникации***;<br>*Нейросети в дизайне***;<br>UX;<br>Основы программирования на Java;<br>Автоматизация бизнес-процессов;<br>Аналитика данных (BI);<br>Компьютерная графика;<br>SQL-программирование; |
| ПК-1 | Способность осуществлять тактическое планирование деятельности структурных подразделений производственной организации | Основы веб-дизайна;<br>Основы дизайна;<br>Основы веб-разработки;<br>Ознакомительная практика; | Эконометрика;<br>Дизайн мобильных приложений;<br>Основы геймдизайна;<br>*Управление разработкой программного обеспечения***;<br>*Управление цифровой трансформацией***;<br>*Архитектура программного обеспечения***;<br>*Рынки ИКТ и организация продаж***;<br>*Технологии искусственного интеллекта***;<br>*Личный бренд и лидерство***;<br>Преддипломная практика;<br>Производственно- |

| Шифр | Наименование компетенции | Предшествующие дисциплины/модули, практики* | Последующие дисциплины/модули, практики* |
|---|---|---|---|
| | | | 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 информационной безопасности» 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 | Теоретические основы информационной безопасности | 1.1 | Основные понятия и задачи информационной безопасности | Вводятся ключевые понятия: конфиденциальность, целостность, доступность (триада CIA), а также угрозы, уязвимости, риски. Рассматриваются задачи обеспечения безопасности веб-проектов: защита пользовательских данных, безопасность API, предотвращение утечек дизайн-макетов и коммерческой информации. | ЛК, СЗ |
| | | 1.2 | Основы защиты информации | Изучаются базовые механизмы защиты: идентификация и аутентификация, управление доступом, шифрование. В контексте веб-разработки разбираются HTTPS, хеширование паролей, многофакторная аутентификация для админ-панелей и систем управления контентом. | ЛК, СЗ |
| | | 1.3 | Угрозы безопасности защищаемой информации | Классификация угроз: вредоносное ПО, социальная инженерия, DDoS-атаки, инсайдерские угрозы. Особое внимание уделяется типовым уязвимостям веб-приложений (OWASP Top 10) – инъекции, XSS, CSRF – и их влиянию на дизайн и функциональность сайтов. | ЛК, СЗ |
| Раздел 2 | Методология защиты информации | 2.1 | Методологические подходы к защите информации (часть 1) | Рассматриваются организационно-правовые и административные методы: политики безопасности, управление рисками, аудит. Приводятся примеры разработки политики безопасности для команды веб-студии или дизайн-агентства: регламенты доступа к репозиториям, требования к паролям, инцидент-менеджмент. | ЛК, СЗ |
| | | 2.2 | Методологические подходы к защите информации (часть 2) | Изучаются программно-технические методы: межсетевые экраны, антивирусная защита, системы обнаружения вторжений. В контексте веб-разработки – настройка WAF (Web Application Firewall), защита от ботов, использование безопасных библиотек и фреймворков. | ЛК, СЗ |
| | | 2.3 | Защита информации в автоматизированных (информационных) системах | Изучаются средства мониторинга, логирования и реагирования на инциденты. Особое внимание уделяется применению технологий искусственного интеллекта и машинного обучения для обнаружения аномалий в сетевом трафике, выявления вторжений (NIDS на основе ML), анализа поведения пользователей (UEBA) и автоматической блокировки | ЛК, СЗ |

| Номер раздела | Наименование раздела дисциплины | Наименование темы | | Содержание темы | Вид учебной работы* |
|---|---|---|---|---|---|
| | | | | подозрительных запросов к веб-приложениям. Рассматриваются примеры использования библиотек Python (scikit-learn, TensorFlow) для построения простых моделей обнаружения атак типа SQL-инъекций или брутфорса | |
| | | 2.4 | Искусственный интеллект в задачах информационной безопасности | Обзор современных ИИ-инструментов для анализа угроз, распознавания вредоносного ПО, защиты веб-форм от автоматических атак (CAPTCHA, поведенческие модели). Практическое занятие: использование готовых моделей для фильтрации спама или детекции фишинговых сайтов. | ЛК, СЗ |
| Раздел 3 | Основы государственной политики Российской Федерации в области информационной безопасности | 3.1 | Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Интересы государства в информационной сфере | Рассматривается доктрина информационной безопасности РФ, стратегические цели. Для специалистов по веб-разработке важно понимание требований к хранению персональных данных граждан РФ (152-ФЗ), локализации серверов, маркировки интернет-ресурсов. | ЛК, СЗ |
| | | 3.2 | Основные составляющие национальных интересов Российской Федерации в информационной сфере. Виды угроз информационной безопасности Российской Федерации | Анализируются угрозы на государственном уровне: кибершпионаж, пропаганда, атаки на критическую инфраструктуру. Проводится параллель с защитой коммерческих веб-проектов от целенаправленных атак и утечек баз данных. | ЛК, СЗ |
| | | 3.3 | Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз | Изучаются источники угроз: иностранные спецслужбы, киберпреступные группы, недобросовестные сотрудники. Обсуждаются меры противодействия при разработке и сопровождении веб-систем: контроль доступа, шифрование, резервное копирование. | ЛК, СЗ |
| | | 3.4 | Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности | Рассматриваются меры государственного регулирования: лицензирование, сертификация средств защиты, создание центров мониторинга. Для веб-разработчика важно понимание требований к безопасности государственных и муниципальных сайтов (ФЗ № 44, приказы Минцифры). | 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. | Операционная система Microsoft Windows, Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010<br>Браузер Яндекс или Mozilla Firefox или Google Chrome<br>Adobe Reader XI или Adobe Acrobat Reader |
| 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. | Операционная система Microsoft Windows, Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010<br>Браузер Яндекс или Mozilla Firefox или Google Chrome<br>Adobe Reader XI или Adobe Acrobat Reader |
| 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. | Операционная система Microsoft Windows, Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010<br>Браузер Яндекс или Mozilla Firefox или Google Chrome<br>Adobe Reader XI или Adobe Acrobat Reader |

* - 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, 2025. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568708

2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/569267

*Дополнительная литература:*

1. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567672

2. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567915

*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 информационной безопасности».

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

**РАЗРАБОТЧИК:**

| Старший преподаватель | | Рожков Андрей Павлович |
|---|---|---|
| *Должность, БУП* | *Подпись* | *Фамилия И.О.* |

**РУКОВОДИТЕЛЬ БУП:**

| Заведующий кафедрой | | Кокуйцева Татьяна Владимировна |
|---|---|---|
| *Должность БУП* | *Подпись* | *Фамилия И.О.* |

**РУКОВОДИТЕЛЬ ОП ВО:**

| Заведующий кафедрой | | Кокуйцева Татьяна Владимировна |
|---|---|---|
| *Должность, БУП* | *Подпись* | *Фамилия И.О.* |