

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 02.05.2026 18:01:51

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a989dae18a

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский университет дружбы народов имени Патриса Лумумбы»

Институт мировой экономики и бизнеса

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

38.03.01 ЭКОНОМИКА

(код и наименование направления подготовки/специальности)

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

БИЗНЕС-КОНСАЛТИНГ, ЦИФРОВОЙ УЧЕТ И АУДИТ

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» входит в программу бакалавриата «Бизнес-консалтинг, цифровой учет и аудит» по направлению 38.03.01 «Экономика» и изучается в 6 семестре 3 курса. Дисциплину реализует Институт мировой экономики и бизнеса. Дисциплина состоит из 5 разделов и 10 тем и направлена на изучение теоретических и практических основ информационной безопасности.

Целью освоения дисциплины является ознакомление студентов с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей, и методов их применения.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Информационная 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-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 Осуществлять 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; УК-12.3 Использует качественные информационные ресурсы, соблюдая требования безопасности, этических и правовых норм, цифровую гигиену;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Информационная безопасность» 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 «Информационная 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-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	<p><i>Налоговые правоотношения в учете**;</i> <i>Экономическая безопасность**;</i> <i>Комплаенс документации**;</i> <i>Электронный документооборот**;</i> <i>Анализ внешней среды бизнеса**;</i> <i>Управление проектами**;</i> Цифровая грамотность; Python для бизнес-аналитики;</p>	<p>Преддипломная практика; <i>Экологический консалтинг и аудит**;</i> <i>Учетные инструменты зеленой экономики**;</i> Искусственный интеллект в учете и аудите;</p>

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Информационная 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)
			6
<i>Контактная работа, ак.ч.</i>	51		51
Лекции (ЛК)	17		17
Лабораторные работы (ЛР)	34		34
Практические/семинарские занятия (СЗ)	0		0
<i>Самостоятельная работа обучающихся, ак.ч.</i>	48		48
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	9		9
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	Введение в информационную безопасность	1.1	Основные понятия, цели и задачи информационной безопасности	В рамках темы рассматривается предмет и объект изучения дисциплины, определяется понятие информационной безопасности как состояния защищённости информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий. Анализируются ключевые цели обеспечения безопасности: конфиденциальность, целостность и доступность информации. Описывается место информационной безопасности в системе национальной и экономической безопасности, а также её роль в деятельности современных организаций.	ЛК, ЛР
		1.2	Угрозы и уязвимости информационных систем	Тема посвящена классификации угроз информационной безопасности, включая естественные, искусственные, случайные и преднамеренные. Рассматриваются основные виды уязвимостей технических, программных и организационных средств, создающих предпосылки для реализации угроз. Анализируются модели нарушителя и источники потенциальных атак, а также методы оценки рисков.	ЛК, ЛР
Раздел 2	Правовые и организационные основы защиты информации	2.1	Нормативно-правовое регулирование в области информационной безопасности	В этом разделе изучается законодательная база Российской Федерации, регулирующая отношения в сфере защиты информации. Рассматриваются основные федеральные законы, указы Президента и постановления Правительства, а также отраслевые стандарты и международные нормативные акты. Особое внимание уделяется вопросам лицензирования деятельности, сертификации средств защиты и ответственности за правонарушения в информационной сфере.	ЛК, ЛР
		2.2	Организационные меры и политика безопасности	Тема охватывает вопросы построения системы управления информационной безопасностью (СУИБ) на предприятии. Изучаются принципы разработки, внедрения и сопровождения политики информационной безопасности как основного документа, регламентирующего правила работы с защищаемыми активами. Рассматриваются организационные процедуры: управление доступом, физическая защита объектов, обучение персонала и планирование непрерывности бизнеса.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 3	Технические средства и методы защиты информации	3.1	Идентификация, аутентификация и управление доступом	В рамках темы изучаются фундаментальные механизмы контроля доступа к ресурсам информационных систем. Рассматриваются методы идентификации и аутентификации пользователей (парольные системы, биометрия, токены), а также модели и политики разграничения доступа, направленные на реализацию принципа минимальных привилегий.	ЛК, ЛР
		3.2	Криптографические методы защиты информации	Тема посвящена изучению математических методов обеспечения конфиденциальности и целостности данных. Рассматриваются классические симметричные и асимметричные алгоритмы шифрования, принципы работы хеш-функций, электронная цифровая подпись (ЭЦП) и инфраструктура открытых ключей (PKI). Анализируются области применения криптографии для защиты каналов связи и хранения информации.	ЛК, ЛР
Раздел 4	Защита сетей и информационных систем	4.1	Сетевая безопасность и защита периметра	В этом разделе рассматриваются угрозы, специфичные для сетевой инфраструктуры. Изучаются принципы работы межсетевых экранов (firewalls), систем обнаружения и предотвращения вторжений (IDS/IPS), а также технологии построения защищённых виртуальных частных сетей (VPN). Анализируются методы сегментации сетей для локализации потенциальных атак.	ЛК, ЛР
		4.2	Защита операционных систем и прикладного ПО	Тема охватывает вопросы обеспечения безопасности на уровне операционных систем (Windows, Linux) и приложений. Рассматриваются механизмы управления обновлениями (patch management), настройка параметров безопасности, использование средств антивирусной защиты и систем контроля целостности файлов для противодействия вредоносному программному обеспечению.	ЛК, ЛР
Раздел 5	Управление инцидентами и современные угрозы	5.1	Мониторинг безопасности и реагирование на инциденты	В рамках темы изучается жизненный цикл управления инцидентами информационной безопасности: от обнаружения подозрительной активности до анализа последствий и восстановления систем. Рассматриваются функции центров мониторинга безопасности (SOC), методы форензики (компьютерной криминалистики) и разработка планов реагирования.	ЛК, ЛР

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		5.2	Современные угрозы: вредоносное ПО, социальная инженерия и DDoS-атаки	Тема посвящена анализу актуальных векторов атак. Подробно рассматриваются типы вредоносного программного обеспечения (вирусы, трояны, шифровальщики), методы социальной инженерии, направленные на манипуляцию людьми, а также принципы организации распределённых атак типа «отказ в обслуживании» (DDoS) и методы противодействия им.	ЛК, ЛР

* - 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.	Комплект специализированной мебели, Экран настенный с электроприводом CactusMotoExpert 150x200см (CS-PSME-200X150-WT), Проектор BenQ MH550, Микроскопы Биомед 4, Микмед 5, МБС 10, Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в том числе MS Office/ Office 365, Teams)
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве ____ шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Microsoft Office 2021 LTSC, Моноблок Digma Pro Unity i7 1255U MHz/16 GB/512 GB/DVD/audio, монитор 27", Мультимедиа проектор Cactus CSC4.SG , Экран моторизованный Digis Electra 200*150 Dsem-4303
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.	Комплект специализированной мебели, Экран настенный с электроприводом CactusMotoExpert 150x200см (CS-PSME-200X150-WT), Проектор BenQ MH550, Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в том числе MS Office/ Office 365, Teams)

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО!**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340>

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: 20.04.2026).

Дополнительная литература:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542339>

2. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544965>

- Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2024. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/545066>

- Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2024. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/545066>

- Козырь, Н. С. Экономические аспекты информационной безопасности : учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва : Издательство Юрайт, 2024. — 131 с. — (Высшее образование). — ISBN 978-5-534-17863-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/545066>

- Лихолетов, В. В. Стратегические аспекты экономической безопасности : учебное пособие для вузов / В. В. Лихолетов. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 201 с. — (Высшее образование). — ISBN 978-5-534-13505-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543772>

- Милешко, Л. П. Экономика и менеджмент безопасности : учебное пособие для среднего профессионального образования / Л. П. Милешко. — Москва : Издательство Юрайт, 2024. — 99 с. — (Профессиональное образование). — ISBN 978-5-534-18899-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/555038>

- Пименов, Н. А. Управление финансовыми рисками в системе

экономической безопасности : учебник и практикум для вузов / Н. А. Пименов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 353 с. — (Высшее образование). — ISBN 978-5-534-16342-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535920>

- Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 427 с. — (Высшее образование). — ISBN 978-5-534-18043-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/535625>

- Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542739>

3. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/588515> (дата обращения: 20.04.2026).

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/>

- 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 «Информационная безопасность».

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

РАЗРАБОТЧИК:

Доцент

Должность, БУП

Подпись

Главина Софья
Григорьевна

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Должность БУП

Подпись

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Доцент

Должность, БУП

Подпись

Абуева Милана Магомед-
Салиевна

Фамилия И.О.