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

Институт мировой экономики и бизнеса экономического факультета

(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 основнойпрофессиональной образовательной программы высшего образования (ОП ВО):

Мировая экономика, Международная экономическая безопасность, Цифроваяэкономика
(наименование (профиль/специализация) ОП ВО)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность» - 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 числеаппаратно-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:

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 УК-12.3. Использует качественные информационные ресурсы, соблюдая требования безопасности, этических иправовых норм, цифровую гигиену

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Информационная безопасность» относится к *вариативной* компоненте блока Б1.В.ДВ.09.01.

В рамках ОП ВО 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	Эконометрика Цифровая грамотность Финансовая безопасность	Модели искусственного интеллекта в арсенале менеджера Инструментальные средства бизнес-аналитики Аналитика социальных медиа для рекламы и PR Сторителлинг в цифровой среде Influence-маркетинг Технологии презентации и переговоров IT-системы E-commerce Информационно-психологическая безопасность Подготовка к сдаче и сдача государственного экзамена Подготовка к процедуре защиты и защита выпускной работы бакалавра Научный семинар Технологии и практика программирования на языке Python для гуманитарных специальностей

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Информационная безопасность»составляет 3 зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО для ***ОЧНОЙ*** *формы обучения*

Вид учебной работы		ВСЕГО, ак.ч.	Семестр(-ы)			
			6			
Контактная работа, ак.ч.		**51**	**51**			
В том числе:						
Лекции(**ЛК**)		17	17			
Лабораторные работы *(***ЛР***)*		34	34			
Практические/семинарские занятия (**СЗ**)		-	-			
Самостоятельная работа обучающихся, ак.ч.		48	48			
Контроль (экзамен/зачет с оценкой), ак.ч.		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

Наименование раздела дисциплины	**Содержание раздела (темы)**	**Вид учебной работы***
Раздел 1 Современное состояние и правовое регулирование сферы информационной безопасности	**Тема 1.1.** Понятие информационной безопасности. Цели обеспечения информационной безопасности. Основные задачи, решаемые при обеспечении информационной безопасности. Законодательные основы по защите информации (Федеральный закон "Об информации, информатизации и защите информации", Закон "О коммерческой тайне", Закон "О банках и банковской деятельности в РФ"и др.). Цели защиты информации. Атака на информацию. Экономические и моральные последствия атаки на информацию.	ЛК, ЛР
	Тема 1.2. Пять уровней обеспечения информационной безопасности (системы защиты): Законодательный, Морально-этический, Административный, Физический, Аппаратно-программный. Основные принципы выстраивания надежной системы защиты.	
	Тема 1.3. Законодательство Российской Федерации и иностранных государств в области информационной безопасности. Конституционные гарантии прав граждан на информацию и механизм их реализации. Понятие и виды защищаемой информации по законодательству Российской Федерации. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны.	ЛК, ЛР
	Тема 1.4. Международное законодательство в области защиты информации. Стандарты в области информационной безопасности. Международные стандарты информационного обмена.	
Раздел 2 Угрозы информационной безопасности и методы их реализации	**Тема 2.1.** Модели оценки ценности информации. Классификация и общий анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения конфиденциальности, целостности и доступности информации.	ЛК, ЛР
	Тема 2.2. Модель нарушителя. Угрозы секретности (конфиденциальности) информации: разглашение, утечка,	

	несанкционированный доступ.	
	Информационная безопасность в условиях функционирования глобальных сетей.	
	Тема 2.3. Понятие компьютерного вируса. История появления компьютерных вирусови факторы, влияющие на их распространение. Вирусы как класс вредоносного программного обеспечения. Классификация компьютерных вирусов.	ЛК, ЛР
	Тема 2.4. Компьютерная преступность. Классификация компьютерных преступлений. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак.	
Раздел 3 Место информационной безопасности экономических систем в национальной безопасности страны	**Тема 3.1.** Схема построения информационной безопасности на уровне государства. Информационная безопасность страны. Защита экономических систем. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.	ЛК, ЛР
	Тема 3.2. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере.	
	Тема 3.3. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.	ЛК, ЛР
	Тема 3.4. Основные положения государственной политики обеспечения информационной безопасности иностранных государств. Доктрина информационной безопасности Российской Федерации. Система обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в правоохранительных органах.	
Раздел 4 Способы и средства обеспечения защиты информации	**Тема 4.1.** Сущность и перечень организационных мер по защите информации. Субъекты деятельности по защите информации. Структура и задачи	ЛК, ЛР
	подразделения по защите информации.	

	Тема 4.2. Сущность и перечень инженерно-технических мер по защите информации. Методика и средства защиты информации. Средства контроля эффективности защиты информации. Средства физической защиты информации.	
	Тема 4.3. Классификация программных средств защиты информации. Использование программ для обеспечения безопасности конфиденциальной информации. Технологии защиты программного обеспечения.	ЛК, ЛР
	Тема 4.4. Защита информации от утечки, несанкционированного доступа и несанкционированного воздействия. Защита информации от непреднамеренного воздействия, разглашения и разведки. Аудит информационной безопасности. Управление рисками.	
Раздел 5 Информационная безопасность прикладных систем	**Тема 5.1.** Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Угрозы информационно- программному обеспечению вычислительных систем и их классификация. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы. Организационная структура системы комплексной защиты информационно-программного обеспечения. Общие сведения о реализациизащиты информационно-программного обеспечения в операционных системах.	ЛК, ЛР
	Тема 5.2. Основные подходы к построению защищенной операционной системы. Административные меры защиты. Виды уязвимости и атак на операционные системы. Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого и динамически изменяющегося паролей. Способы разграничения доступа к компьютерным ресурсам. Защита программных средств от несанкционированного копирования, исследования и модификации. Защита офисных документов. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.	

	Тема 5.3. Общая организация защиты от компьютерных вирусов. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.Программные средства обслуживания операционных систем. Утилиты и специализированные программы профилактики компьютера. Программные средства восстановления информации. Защита электронных запоминающих устройств.	
Раздел 6 Безопасность компьютерных сетей	**Тема 6.1.** Компьютерные сети, топология сетей, структура Интернет. Принципы передачи информации в сети (протокол TCP/IP, доменная система имен, пакеты, порты, сетевые службы). Принципы работы традиционных механизмов защиты компьютерных сетей. Организация защиты от несанкционированного доступа.	ЛК, ЛР
	Тема 6.2. Защита Интернет-подключений. Функции межсетевых экранов, понятие брандмауэра. Технологии межсетевых экранов (фильтрация пакетов, применение шлюзов, прочие компоненты брандмауэров (файрволлов). Брандмауэр Windows, настройка и определение правил. Журналы доступа. Выявление следов несанкционированного доступа к файлам. Сканеры и автоматизация поиска слабых мест в защите сети и в защите системы. Анализаторы протоколов.	
	Тема 6.3. Возможности выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий. Противодействие распространению наркотиков в сетиИнтернет.	
Раздел 7 Криптографическаязащита информации	**Тема 7.1.** Криптография, Криптоанализ. Основные понятия криптологии. История шифрования.	ЛК, ЛР
	Тема 7.2. Использование шифрования различными методами. Симметричные и несимметричные системы шифрования информации. Рассмотрение сокрытия	
	информации таблицей Винжера. Программы для криптографии. Криптографические алгоритмы.	
	Тема 5.3. Электронная цифровая подпись (ЭЦП) и функция хэширования. Создание и использование криптоключей. Подтверждение подлинности объектов и субъектов информационной системы.	

	Тема 7.4. Понятие криптографической стойкости, вопросы практической стойкости. Программно-аппаратные средства криптозащиты данных.	

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)
Специализированная аудитория	Аудитория для проведения лекций и семинарских занятий, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебелии оборудованием. (аудитории327, 330, 333)	Комплект специализированной мебели, Экран настенный с электроприводом CactusMotoExpert 150x200см (CS-PSME-200X150-WT), Проектор BenQ MH550,МикроскопыБиомед 4, Микмед 5, МБС 10, Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в том числе MS Office/ Office 365, Teams)
Для самостоятельной работы обучающихся	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарский занятий и консультаций), оснащенная комплектом специализированной мебели (аудитория 18)	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)

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

Электронные и печатные полнотекстовые материалы:

1. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный //Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002 (датаобращения: 24.05.2022).

2. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов /Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741 (дата обращения: 24.05.2022).

3. *Внуков, А. А.* Защита информации : учебное пособие для вузов /А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный //Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 24.05.2022). *Чернова, Е. В.* Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный
// Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495922 (дата обращения: 24.05.2022).

Дополнительная литература:
Электронные и печатные полнотекстовые материалы:

1. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 24.05.2022).
2. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательнаяплатформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019 (дата обращения: 24.05.2022).
3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534- 03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 24.05.2022).
4. *Запечников, С. В.* Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487 (дата обращения: 24.05.2022).

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеютдоступ на основании заключенных договоров:
– Электронно-библиотечная система РУДН – ЭБС РУДН http://lib.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 «Лань» http://e.lanbook.com/
2. Базы данных и поисковые системы:
– NCBI: https://p.360pubmed.com/pubmed/
– Вестник РУДН: режим доступа с территории РУДН и удаленно http://journals.rudn.ru/
– Научная библиотека Elibrary.ru: доступ по IP-адресам РУДН по адресу:http://www.elibrary.ru/defaultx.asp
– ScienceDirect (ESD), «FreedomCollection», "Cell Press" ИД "Elsevier"**.** Есть удаленный доступ к базе данных, доступ по IP-адресам РУДН (или удаленно по индивидуальномулогину и паролю).
– Академия Google (англ. Google Scholar) - бесплатная поисковая система по полнымтекстам научных публикаций всех форматов и дисциплин.
Индексирует полные тексты научных публикаций. Режимдоступа: https://scholar.google.ru/
– Scopus - наукометрическая база данных издательства ИД "Elsevier". Доступ на платформу осуществляется по IP-адресам РУДН или удаленно. http://www.scopus.com/
– Web of Science. Доступ на платформу осуществляется по IP-адресам РУДН илиудаленно. http://login.webofknowledge.com/

Учебно-методические материалы для самостоятельной работы обучающихсяпри освоении дисциплины/модуля:*

1. Методические указания для обучающихся по освоению дисциплины «**Информационная безопасность**»
2. Лекционный материал
* - все учебно-методические материалы для самостоятельной работы обучающихся

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИКОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «**Информационная безопасность**» представлены в Приложении к настоящей Рабочей программе дисциплины.

* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.

РАЗРАБОТЧИКИ:

старший преподаватель		**Гусев А.И.**
Должность, БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

К.э.н., доцент, Руководитель программы «Международная экономическая безопасность»		**Глинская М.В.**
Должность, БУП	Подпись	Фамилия И.О.

Руководитель программы «Мировая экономика»		**Айдрус И.А.З.**
Должность, БУП	Подпись	Фамилия И.О.

Руководитель программы «Цифровая экономика»		**Главина С.Г.**
Должность, БУП	Подпись	Фамилия И.О.