

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 06.2023.14.21.01
Уникальный программный ключ:
ca953a0120d891083f939673078ef1a989dae18a

**Федеральное государственное автономное образовательное учреждение
высшего образования «Российский университет дружбы народов»**

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):

Мировая экономика, Международная экономическая безопасность, Цифровая экономика

(наименование (профиль/специализация) ОП ВО)

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 числе аппаратно-программных, используемых для этих целей, 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 к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм | 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 и правовых норм, цифровую гигиену |
| ОПК - 2 | Способен осуществлять сбор, обработку и статистический анализ данных, необходимых для решения поставленных экономических задач | ОПК-2.1. Определяет методы сбора информации, способы и вид ее представления, применяя современное программное обеспечение ОПК-2.2. Выбирает соответствующие содержанию профессиональных задач инструментарий обработки и анализа данных, современные информационные ОПК-2.3. Осуществляет визуализацию данных и презентацию решений в информационной среде |
| ОПК - 5 | Способен использовать современные информационные технологии и программные средства при решении профессиональных задач | ОПК-5.1. Применяет как минимум один из общих или специализированных пакетов прикладных программ (таких как MS Excel, Eviews, Stata, SPSS, R и др.), предназначенных для выполнения статистических процедур (обработка статистической информации, построение и проведение диагностики эконометрических моделей) ОПК-5.2. Использует электронные библиотечные системы для поиска необходимой научной литературы и |

| | | |
|------|---|---|
| | | социально-экономической статистики ОПК-5.3. Решает профессиональные задачи с применением необходимого программного обеспечения и информационных технологий |
| ПК-1 | Способен анализировать и интерпретировать данные отечественной и зарубежной статистики о социально-экономических процессах и явлениях, выявлять тенденции изменения социально-экономических показателей | ПК-1.1. Знает методы анализа и интерпретации данных статистики о социально-экономических процессах и явлениях ПК-1.2. Умеет на основе анализа выделять тенденции изменения социально-экономических показателей ПК-1.3. Ориентируется в актуальных тенденциях социально-экономического развития мира |

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «**Информационная безопасность**» относится к *вариативной* компоненте блока Б1.О.02.09.

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 к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм | Микроэкономика Макроэкономика | Международные экономические отношения Преддипломная практика Производственная практика |
| ОПК - 2 | Способен осуществлять сбор, обработку и статистический анализ данных, необходимых для решения поставленных экономических задач | Микроэкономика Макроэкономика | Международные экономические отношения Преддипломная практика Производственная практика |
| ОПК - 5 | Способен использовать современные информационные технологии и программные средства при решении | Микроэкономика Макроэкономика | Международные экономические отношения Преддипломная практика Производственная практика |

| | | | |
|-------|---|----------------------------------|---|
| | профессиональных задач | | |
| ПК-1 | Способен анализировать и интерпретировать данные отечественной и зарубежной статистики о социально-экономических процессах и явлениях, выявлять тенденции изменения социально-экономических показателей | Микроэкономика Макроэкономика | Международные экономические отношения Преддипломная практика Производственная практика |
| УК-12 | Способен к взаимодействию в условиях современной информационной культуры и цифровой экономики с учетом требований информационной безопасности, этических и правовых норм | Микроэкономика Макроэкономика | Мировая экономика Международные экономические отношения Преддипломная практика Производственная практика |

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

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) | | | |
|---|-----------------|-------------|-----|--|--|
| | | 3 | | | |
| Контактная работа, ак.ч. | 34 | 34 | | | |
| В том числе: | | | | | |
| Лекции(ЛК) | 17 | 17 | | | |
| Лабораторные работы (ЛР) | | | | | |
| Практические/семинарские занятия (СЗ) | 17 | 17 | | | |
| Самостоятельная работа обучающихся, ак.ч. | 47 | 47 | | | |
| Контроль (экзамен/зачет с оценкой), ак.ч. | 27 | 27 | | | |
| 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* |
|---|---|---------------------|
| <p>Раздел 1 Современное состояние и правовое регулирование сферы информационной безопасности</p> | <p>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.</p> | ЛК, СЗ |
| | <p>Тема 1.2. Пять уровней обеспечения информационной безопасности (системы защиты): Законодательный, Морально-этический, Административный, Физический, Аппаратно-программный. Основные принципы выстраивания надежной системы защиты.</p> | |
| | <p>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.</p> | ЛК, СЗ |
| | <p>Тема 1.4. Международное законодательство в области защиты информации. Стандарты в области информационной безопасности. Международные стандарты информационного обмена.</p> | |
| <p>Раздел 2 Угрозы информационной безопасности и методы их реализации</p> | <p>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.</p> | ЛК, СЗ |
| <p>Тема 2.2. Модель нарушителя. Угрозы секретности (конфиденциальности) информации: разглашение, утечка, несанкционированный доступ.</p> | | |

| | | |
|--|---|--------|
| | Информационная безопасность в условиях функционирования глобальных сетей. | |
| | Тема 2.3. Понятие компьютерного вируса. История появления компьютерных вирусов и факторы, влияющие на их распространение. Вирусы как класс вредоносного программного обеспечения. Классификация компьютерных вирусов. | ЛК, СЗ |
| | 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, СЗ |
| | 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, СЗ |
| | 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, СЗ |

| | | |
|--|--|--------|
| | <p>подразделения по защите информации.</p> | |
| | <p>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.</p> | |
| | <p>Тема 4.3. Классификация программных средств защиты информации. Использование программ для обеспечения безопасности конфиденциальной информации. Технологии защиты программного обеспечения.</p> | ЛК, СЗ |
| | <p>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.</p> | |
| <p>Раздел 5 Информационная безопасность прикладных систем</p> | <p>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 реализации защиты информационно-программного обеспечения в операционных системах.</p> | ЛК, СЗ |
| | <p>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,</p> | |

| | | |
|--|---|--------|
| | <p>исследования и модификации. Защита офисных документов. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.</p> <p>Тема 5.3. Общая организация защиты от компьютерных вирусов. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Технология гарантированного восстановления 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.</p> | |
| <p>Раздел 6 Безопасность компьютерных сетей</p> | <p>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.</p> | ЛК, СЗ |
| | <p>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.</p> | |
| | <p>Тема 6.3. Возможности выявления и раскрытия преступлений в сфере компьютерной информации и высоких технологий. Противодействие распространению наркотиков в сети Интернет.</p> | |
| <p>Раздел 7 Криптографическая защита информации</p> | <p>Тема 7.1. Криптография, Криптоанализ. Основные понятия криптологии. История шифрования.</p> | ЛК, СЗ |
| | <p>Тема 7.2. Использование шифрования различными методами. Симметричные и несимметричные системы шифрования информации. Рассмотрение сокрытия</p> | |

| | | |
|--|--|--|
| | 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. | |

* - заполняется только по **ОЧНОЙ** форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – 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) |
|--|---|---|
| Специализированная аудитория | Аудитория для проведения лекций и семинарских занятий, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и оборудованием. (аудитории 327, 330, 333) | Комплект специализированной мебели, Экран настенный с электроприводом CactusMotoExpert 150x200см (CS-PSME-200X150-WT), Проектор BenQ МН550, Микроскопы Биомед 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 семинарских занятий и консультаций), оснащенная комплектом специализированной мебели (аудитория 18) | Комплект специализированной мебели, Экран настенный с электроприводом CactusMotoExpert 150x200см (CS-PSME-200X150-WT), Проектор BenQ МН550, 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:

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> (дата обращения: 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 // Образовательная платформа 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 имеют доступ 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 индивидуальному логину и паролю).
- Академия Google (англ. Google Scholar) - бесплатная поисковая система по полным текстам научных публикаций всех форматов и дисциплин. Индексирует полные тексты научных публикаций. Режим доступа: <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 или удаленно. <http://login.webofknowledge.com/>

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

1. Методические указания для обучающихся по освоению дисциплины «Информационная безопасность»

2. Лекционный материал

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

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ 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 ИМЭБ

Должность, БУП

Подпись

Гусев А.И.

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Декан

Наименование БУП

Подпись

Мосейкин Ю.Н.

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Руководитель программы
«Мировая экономика»

Должность, БУП



Подпись

Айдрус И.А.З.

Фамилия И.О.