

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 03.05.2026 14:02:29

Уникальный программный ключ:

sa953a0120d891083f939673078ef1a989dae18a

**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):**

#### **МИРОВАЯ ЭКОНОМИКА И МЕЖДУНАРОДНАЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ**

(наименование (профиль/специализация) ОП ВО)

**2026 г.**

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» входит в программу бакалавриата «Мировая экономика и международная экономическая безопасность» по направлению 38.03.01 «Экономика» и изучается в 6 семестре 3 курса. Дисциплину реализует Институт мировой экономики и бизнеса. Дисциплина состоит из 7 разделов и 16 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<br>(в рамках данной дисциплины)  |
|------|--|--|
| ПК-1 | Способен, используя отечественные и зарубежные источники информации, собирать необходимые данные, анализировать их и готовить информационные обзоры и аналитические отчеты для решения задач профессиональной деятельности | ПК-1.1 Осуществляет поиск информации для решения, поставленной задачи профессиональной деятельности;<br>ПК-1.2 Анализирует и контекстно обрабатывает информацию для решения поставленных профессиональных задач;<br>ПК-1.3 Обобщает, обосновывает и готовит информационные обзоры и аналитические отчеты для решения задач профессиональной деятельности;  |
| ПК-4 | Способен анализировать большие данные с использованием современной методологической и технологической инфраструктуры   | ПК-4.1 Выявляет, формирует и согласует требования к результатам аналитических работ с применением технологий больших данных;<br>ПК-4.2 Планирует и организует аналитические работы с использованием технологий больших данных;<br>ПК-4.3 Подготавливает данные для проведения аналитических работ по исследованию больших данных;<br>ПК-4.4 Проводит аналитические исследования с применением технологий больших данных в соответствии с требованиями заказчика; |

## 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*   |
|------|--|--|--|
| ПК-1 | Способен, используя отечественные и зарубежные источники информации, собирать необходимые данные, анализировать их и готовить информационные обзоры и аналитические отчёты для решения задач профессиональной деятельности | <p><i>Экономика и политика стран Латинской Америки**;</i><br/> Налоги и налогообложение;<br/> Мировой рынок труда и международная миграция;<br/> Зарубежное страноведение;<br/> Процессы региональной экономической интеграции в мировой экономике;<br/> Анализ и прогноз мировых рынков товаров и услуг;<br/> <i>Миграционные режимы и паспортно-визовая дипломатия**;</i><br/> Маркетинг;<br/> Экономическая география;<br/> <i>Свободные экономические зоны и офшоры**;</i><br/> Международные платежные системы и инструменты;<br/> Международные статистические базы данных;<br/> <i>Глобальные тренды развития мировой промышленности**;</i><br/> <i>Геоэкономический потенциал стран с формирующимися рынками**;</i><br/> <i>Мировые финансовые центры**;</i></p> | <p>Преддипломная практика;<br/> Международные валютно-кредитные отношения;<br/> Основы таможенно-тарифного регулирования;<br/> <i>Страны Большой семерки в мировой экономике**;</i><br/> <i>БРИКС+ в мировой экономике**;</i><br/> <i>Международная торговля интеллектуальной собственностью и высокотехнологичной продукцией**;</i><br/> <i>Инвестиционные стратегии транснациональных корпораций в странах Африки**;</i></p> |
| ПК-4 | Способен анализировать большие данные с использованием современной методологической и технологической инфраструктуры   | <p><i>Ознакомительная практика;</i></p>  | <p>Преддипломная практика;</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           |
| <b>Общая трудоемкость дисциплины</b>             | <b>ак.ч.</b>   | <b>108</b> | <b>108</b>  |
|  | <b>зач.ед.</b> | <b>3</b>   | <b>3</b>    |

## 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      | Современное состояние и правовое регулирование сферы информационной безопасности | 1.1               | Понятие и правовые основы информационной безопасности   | Раскрываются понятие информационной безопасности, её цели и задачи в контексте экономической деятельности. Анализируется система российского законодательства в области защиты информации, включая Федеральный закон «Об информации, информатизации и защите информации», законы «О коммерческой тайне», «О банках и банковской деятельности», а также иные нормативные акты, регламентирующие правовой режим защищаемой информации. Рассматриваются категории государственной, коммерческой и личной тайны, механизмы реализации конституционных гарантий прав граждан на информацию, а также экономические и моральные последствия информационных атак. | ЛК, ЛР, СЗ          |
|               |  | 1.2               | Уровни и принципы построения системы защиты информации  | Изучается архитектура системы обеспечения информационной безопасности, включающая законодательный, морально-этический, административный, физический и аппаратно-программный уровни. Формулируются основные принципы выстраивания надёжной системы защиты, учитывающие непрерывность, комплексность, разграничение доступа и минимизацию полномочий. Особое внимание уделяется взаимосвязи организационно-распорядительных мер и технических средств защиты.   | ЛК, ЛР, СЗ          |
|               |  | 1.3               | Отечественное и международное законодательство в области информационной безопасности                          | Проводится сравнительный анализ законодательства Российской Федерации и иностранных государств в сфере защиты информации. Рассматриваются положения Конституции РФ, определяющие права граждан на информацию, и механизмы их реализации. Изучаются международные стандарты информационной безопасности (ISO/IEC 27000, стандарты информационного обмена), а также принципы гармонизации национальных нормативных систем в условиях трансграничного информационного взаимодействия.  | ЛК, ЛР, СЗ          |
| Раздел 2      | Угрозы информационной безопасности и методы их реализации                        | 2.1               | Модели оценки ценности информации. Классификация и общий анализ угроз безопасности информации. Причины, виды, | Раскрываются подходы к оценке ценности информации как актива. Систематизируются угрозы безопасности информации по причинам возникновения, видам и каналам утечки, методам   | ЛК, ЛР, СЗ          |

| Номер раздела | Наименование раздела дисциплины   | Наименование темы |  | Содержание темы   | Вид учебной работы* |
|---------------|---|-------------------|--|---|---------------------|
|               |   |                   | каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения конфиденциальности, целостности и доступности информации. | реализации (нарушение конфиденциальности, целостности, доступности). Рассматривается модель нарушителя, включая классификацию субъектов несанкционированного доступа, мотивацию и потенциальные возможности. Анализируется специфика угроз в условиях функционирования глобальных сетей.  |                     |
|               |   | 2.2               | Компьютерные вирусы и вредоносное программное обеспечение  | Изучается феномен компьютерных вирусов как класса вредоносного программного обеспечения: история возникновения, факторы распространения, классификация по среде обитания, способам заражения и деструктивным функциям. Рассматриваются современные методы противодействия вирусным атакам, а также организационные и технические меры профилактики заражения и восстановления вычислительных систем.  | ЛК, ЛР, СЗ          |
|               |   | 2.3               | Компьютерная преступность и нарушители информационной безопасности   | Анализируется понятие компьютерной преступности, классификация преступлений в сфере информационных технологий. Характеризуются различные категории нарушителей (инсайдеры, хакеры, скрипт-кидди, хактивисты), их мотивация и типовые методы совершения атак. Рассматриваются примеры резонансных хакерских атак, их экономические последствия и способы противодействия.  | ЛК, ЛР, СЗ          |
| Раздел 3      | Место информационной безопасности экономических систем в национальной безопасности страны | 3.1               | Информационная безопасность как фактор устойчивости экономических систем   | В рамках темы анализируется взаимосвязь между уровнем защищённости информационной инфраструктуры хозяйствующих субъектов и обеспечением национальной безопасности государства. Рассматриваются положения Доктрины информационной безопасности Российской Федерации, стратегии развития информационного общества и иных концептуальных документов, определяющих приоритеты защиты критической информационной инфраструктуры. Особое внимание уделяется вопросам цифрового суверенитета, противодействия иностранному информационно-технологическому воздействию и роли экономических систем в поддержании стабильности национального информационного пространства. | ЛК, ЛР, СЗ          |
|               |   | 3.2               | Риски и вызовы информационной безопасности в контексте международной экономической деятельности  | Тема посвящена анализу угроз информационной безопасности, возникающих при интеграции национальных экономических систем в глобальное информационное пространство. Изучаются  | ЛК, ЛР, СЗ          |

| Номер раздела | Наименование раздела дисциплины                  | Наименование темы |  | Содержание темы   | Вид учебной работы* |
|---------------|--|-------------------|--|---|---------------------|
|               |  |                   |  | механизмы воздействия на критическую информационную инфраструктуру со стороны иностранных субъектов, включая промышленный шпионаж, кибератаки на финансовый сектор и трансграничное распространение вредоносного программного обеспечения. Рассматриваются подходы к управлению рисками в условиях санкционных ограничений и политики импортозамещения в сфере информационных технологий.   |                     |
| Раздел 4      | Способы и средства обеспечения защиты информации | 4.1               | Организационные и инженерно-технические меры защиты информации   | В теме раскрывается сущность организационных мер защиты: регламентация доступа, кадровая работа, планирование действий в чрезвычайных ситуациях, создание подразделений по защите информации. Анализируются инженерно-технические средства: физическая защита объектов, системы контроля и управления доступом, средства предотвращения утечки информации по техническим каналам (акустическим, вибрационным, электромагнитным). Рассматриваются методики и средства контроля эффективности защиты, включая аудит информационной безопасности и управление рисками. | ЛК, ЛР, СЗ          |
|               |  | 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 посвящена классификации программных средств защиты информации, их функциональному назначению и архитектуре. Рассматриваются технологии обеспечения безопасности конфиденциальной информации, включая средства антивирусной защиты, системы обнаружения и предотвращения вторжений, средства контроля целостности данных. Анализируются методы защиты программного обеспечения от несанкционированного копирования, исследования и модификации, а также способы защиты офисных документов и привязки программ к среде функционирования.                         | ЛК, ЛР, СЗ          |
| Раздел 5      | Информационная безопасность прикладных систем    | 5.1               | Защита информации в вычислительных системах и операционных средах  | В теме рассматриваются проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах, этапы построения системы комплексной защиты. Изучаются методы идентификации и аутентификации пользователей (простые и динамически изменяемые пароли, биометрические технологии), способы разграничения доступа к ресурсам вычислительной системы. Анализируются виды уязвимостей операционных систем, административные меры   | ЛК, ЛР, СЗ          |

| Номер раздела | Наименование раздела дисциплины     | Наименование темы |   | Содержание темы  | Вид учебной работы* |
|---------------|-------------------------------------|-------------------|---|--|---------------------|
|               |                                     |                   |   | защиты и подходы к защите программных средств от несанкционированного запуска.   |                     |
|               |                                     | 5.2               | Противодействие вредоносному программному обеспечению и восстановление систем | Тема охватывает общую организацию защиты от компьютерных вирусов и иных деструктивных программ. Рассматриваются средства аппаратного и программного контроля, технология гарантированного восстановления вычислительной системы после заражения. Изучаются программные средства обслуживания операционных систем, утилиты профилактики, средства восстановления информации и защиты электронных запоминающих устройств.  | ЛК, ЛР, СЗ          |
| Раздел 6      | Безопасность компьютерных сетей     | 6.1               | Архитектура и уязвимости компьютерных сетей                                   | В теме раскрываются принципы организации компьютерных сетей, топологии, структура сети Интернет. Анализируются основы передачи информации в сетях: протокол TCP/IP, доменная система имён, пакеты, порты, сетевые службы. Рассматриваются традиционные механизмы защиты сетей, организация защиты от несанкционированного доступа и выявление следов несанкционированных действий.   | ЛК, ЛР, СЗ          |
|               |                                     | 6.2               | Технологии защиты сетевых подключений и мониторинга                           | Тема посвящена изучению функций межсетевых экранов (брандмауэров), технологиям фильтрации пакетов, применению шлюзов и иных компонентов. Рассматриваются возможности настройки брандмауэров, ведение журналов доступа, использование сканеров уязвимостей и анализаторов протоколов для автоматизации поиска слабых мест в защите сети и системы. Обсуждаются методы выявления и раскрытия преступлений в сфере компьютерной информации, включая противодействие распространению противоправного контента. | ЛК, ЛР, СЗ          |
| Раздел 7      | Криптографическая защита информации | 7.1               | Основы криптологии и история развития шифрования                              | В теме вводятся основные понятия криптологии (криптография, криптоанализ), рассматривается эволюция методов шифрования от классических до современных. Анализируются симметричные и асимметричные системы шифрования, их сильные стороны и ограничения. Изучается понятие криптографической стойкости и вопросы практической стойкости алгоритмов в условиях развития вычислительных мощностей.  | ЛК, ЛР, СЗ          |
|               |                                     | 7.2               | Криптографические алгоритмы, электронная подпись и инфраструктура             | Тема охватывает применение шифрования различными методами, включая сокрытие информации таблицей Виженера   | ЛК, ЛР, СЗ          |

| Номер раздела | Наименование раздела дисциплины | Наименование темы |        | Содержание темы  | Вид учебной работы* |
|---------------|---------------------------------|-------------------|--------|--|---------------------|
|               |                                 |                   | ключей | и современные криптографические алгоритмы. Рассматриваются принципы формирования и использования электронной цифровой подписи, хэш-функции, процедуры подтверждения подлинности объектов и субъектов информационной системы. Анализируются программно-аппаратные средства криптографической защиты данных, включая генерацию и управление криптоключами. |                     |

\* - 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.   | Мультимедийная доска   |
| Компьютерный класс         | Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве 1 шт.), доской (экраном) 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.  | Мультимедийная доска   |

\* - 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. Войниканис, Е. А. Правовое регулирование информационных отношений в сфере защиты информации с ограниченным доступом : учебное пособие для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 57 с. — (Высшее образование). — ISBN 978-5-534-17204-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544885>

- Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544290> Информационные технологии в экономике и управлении : учебник для вузов / В. В. Трофимов [и др.] ; ответственный редактор В. В. Трофимов. —

4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 556 с. — (Высшее образование). — ISBN 978-5-534-18678-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/545322>

- Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536225>

- Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544029>

*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>

*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](http://www.studentlibrary.ru)

- ЭБС «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации  
<http://docs.cntd.ru/>

- поисковая система Яндекс <https://www.yandex.ru/>

- поисковая система Google <https://www.google.ru/>

- реферативная база данных SCOPUS

<http://www.elsevierscience.ru/products/scopus/>

*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:**

Ассистент кафедры  
международных экономических  
отношений

*Должность, БУП*

*Подпись*

Назарова Дарья  
Валериевна

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ БУП:**

*Должность БУП*

*Подпись*

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ ОП ВО:**

Декан экономического  
факультета

*Должность, БУП*

*Подпись*

Андропова Инна  
Витальевна

*Фамилия И.О.*