

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 27.06.2022 10:46:46
Уникальный программный ключ:
ca953a0120d891083f939673078ef1a989d8e18a

Федеральное государственное автономное образовательное учреждение высшего образования

«Российский университет дружбы народов»

Факультет физико-математических и естественных наук

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Правовые основы кибербезопасности

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки:

38.03.05 Бизнес-информатика

(код и наименование направления подготовки/специальности)

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

Кибербезопасность в экономике

(наименование (профиль/специализация) ОП ВО)

2022 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Правовые основы кибербезопасности» является введение учащихся в предметную область современного права, которая относится к защите частной, государственной, муниципальной и иных форм собственности в киберпространстве, правовой защите объектов обеспечения кибербезопасности, защите прав и законных интересов граждан и юридических лиц в информационной сфере, оказанию юридической помощи, консультированию по вопросам правового обеспечения кибербезопасности, осуществление правовой экспертизы нормативных правовых актов, касающихся деятельности в области обеспечения кибербезопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Правовые основы кибербезопасности» направлено на формирование у обучающихся следующих компетенций (части компетенций): УК-2; ПК-5.

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения.
		УК-2.2. Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности.
		УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ПК-5	Способен решать задачи управления кибербезопасностью предприятий и иных экономических систем.	ПК-5.2. Знает основы нормативно-правового регулирования в РФ и иных странах в области защиты информации.
		ПК-5.4. Умеет использовать нормативно-правовую базу РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем.
		ПК-5.6. Владеет навыками применения нормативно-правовой базы РФ и иных стран в

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Правовые основы кибербезопасности» относится к обязательной части блока Б1 ОП ВО.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Правовые основы кибербезопасности».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики ¹
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	-	Правоведение Кибербезопасность предприятия Экономическая безопасность в современных условиях Теневая экономика Киберполитика в международных экономических отношениях Искусственный интеллект в бизнесе Финансовая безопасность Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности) Преддипломная практика
ПК-5	Способен решать задачи управления кибербезопасностью предприятий и иных экономических систем.		Цифровая трансформация глобальной экономики Международные платежные системы Дизайн мышление Экономическая безопасность в современных условиях Теневая экономика Киберполитика в международных экономических отношениях

¹- заполняется в соответствии с матрицей компетенций и СУП ОП ВО

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики
			<p>Мировая экономика Искусственный интеллект в бизнесе Финансовая безопасность Инновации в бизнесе Кибербезопасность предприятия Источники угроз кибербезопасности Технологии обеспечения кибербезопасности предприятий Противодействие распространению ложной и вредоносной информации в киберпространстве Практическая защита сетей на основе анализа данных Анализ данных и показатели эффективности кибербезопасности предприятия Применение машинного обучения в кибербезопасности Экономическая кибербезопасность Имитационное моделирование угроз экономической кибербезопасности Кибербезопасность платежных систем Экономика "Умного города" и обеспечение безопасности ее функционирования Киберполигон Бизнес-аналитика и методы принятия решений на основе Big Data Технологии распределенного реестра Blockchain Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности) Преддипломная практика</p>

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Правовые основы кибербезопасности» составляет 2 зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы	ВСЕГО, ак.ч.	Семестр(-ы)
		4
Контактная работа, ак.ч.	36	36
Лекции (ЛК)	18	18
Лабораторные работы (ЛР)	-	-
Практические/семинарские занятия (СЗ)	18	18
Самостоятельная работа обучающихся, ак.ч.	36	36
Контроль (экзамен/зачет с оценкой), ак.ч.	-	-
Общая трудоемкость дисциплины	ак.ч.	72
	зач.ед.	2

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы ²
Раздел 1. Введение в правовые основы кибербезопасности.	Тема 1.1. Киберпространство и правовое регулирование в нем. Объекты и субъекты права в киберпространстве.	ЛР, СЗ
	Тема 1.2. Доктринальные основы безопасности личности, экономических субъектов, общества и государства в киберпространстве. Цели, принципы, состояние правового регулирования кибербезопасности.	ЛР, СЗ
	Тема 1.3. Обеспечение правовой кибербезопасности. Виды правонарушений в киберпространстве. Ответственность за правонарушения в киберпространстве.	ЛР, СЗ
Раздел 2. Правовые аспекты преступлений против личности.	Тема 2.1. Правовое обеспечение кибербезопасности личности в киберпространстве. Уголовная и административная защита личности в киберпространстве.	ЛР, СЗ
	Тема 2.2. Нарушение неприкосновенности частной жизни, нарушения тайны переписки, телефонных переговоров. Правонарушения в области обработки персональных данных.	ЛР, СЗ
	Тема 2.3. Угрозы правам и свободам личности в киберпространстве. Экономические преступления против личности в киберпространстве.	ЛР, СЗ

²- заполняется только по ОЧНОЙ форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – семинарские занятия

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
Раздел 3. Правовые аспекты преступлений против частных компаний.	Тема 3.1. Внутренние и внешние киберугрозы интересам частных компаний в киберпространстве. Латентность правонарушений. Правовые условия обеспечения информационной безопасности частных компаний. Недобросовестная конкуренция и кибербезопасность. Объекты защиты в целях обеспечения кибербезопасности частных компаний.	ЛР, СЗ
	Тема 3.2. Защита корпоративной информации. Правовые режимы корпоративной информации (общедоступная информация, информация ограниченного доступа) и организационно-технические средства защиты (ограничение доступа, шифрование). Защита права на доступ к информации, необходимой для ведения бизнеса. Право доступа и условия доступа к корпоративной информации. Защита корпоративных информационных систем и сетей. Требования по защите корпоративных компьютерных систем и сетей в специальных или отраслевых законах. Сочетание права и обязанности при обеспечении кибербезопасности частных компаний.	ЛР, СЗ
	Тема 3.3. Ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области кибербезопасности (применение средств защиты информации, лицензирование отдельных видов деятельности по обеспечению кибербезопасности). Административная и уголовная ответственность за нарушение требований по обеспечению кибербезопасности частных компаний.	ЛР, СЗ
Раздел 4. Правовые аспекты преступлений против государства.	Тема 4.1. Защита интересов государства в киберпространстве. Правовое обеспечение информационного суверенитета Российской Федерации.	ЛР, СЗ
	Тема 4.2. Кибербезопасность при предоставлении электронных государственных и муниципальных услуг, проведении электронных выборов, электронного голосования. Кибербезопасность в системе государственной и муниципальной службы. Организационно-правовые меры обеспечения безопасности открытых данных.	ЛР, СЗ
	Тема 4.3. Правовое регулирование обеспечения кибербезопасности функционирования информационных и телекоммуникационных систем критически важных	ЛР, СЗ

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	объектов инфраструктуры Российской Федерации.	
Раздел 5. Правовые аспекты международных киберпреступлений.	Тема 5.1. Правовые проблемы трансграничности информационно-коммуникационных сетей.	ЛР, СЗ
	Тема 5.2. Установление юрисдикции правонарушителя в условиях глобальных коммуникаций.	ЛР, СЗ
	Тема 5.3. Правовые проблемы обеспечения ответственности за правонарушения в международном киберпространстве.	ЛР, СЗ
Раздел 6. Правовое регулирование в области интеллектуальной собственности	Тема 6.1. Основные понятия в авторском праве.	ЛР, СЗ
	Тема 6.2. Нарушения авторских, изобретательских, патентных прав.	ЛР, СЗ
	Тема 6.3. Защита авторских и смежных прав, ответственность за их нарушение.	ЛР, СЗ

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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Для самостоятельной работы обучающихся	Аудитория 210 для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Калятин, В. О. Право интеллектуальной собственности. Правовое регулирование баз данных : учебное пособие для вузов / В. О. Калятин. — Москва : Издательство Юрайт, 2022. — 186 с. — (Высшее образование). — ISBN 978-5-534-06200-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/493351>.
2. 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>.
3. Зенин, И. А. Право интеллектуальной собственности : учебник для вузов / И. А. Зенин. — 11-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 577 с. — (Высшее образование). — ISBN 978-5-534-15292-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/488195>.
4. Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2022. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496717>.
5. Цифровая криминалистика : учебник для вузов / В. Б. Вехов [и др.] ; под редакцией В. Б. Вехова, С. В. Зуева. — Москва : Издательство Юрайт, 2022. — 417 с. — (Высшее образование). — ISBN 978-5-534-14600-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/497080>.

Дополнительная литература:

1. Волков, Ю. В. Информационное право. Информация как правовая категория : учебное пособие для вузов / Ю. В. Волков. — 2-е изд., стер. — Москва : Издательство Юрайт, 2022. — 109 с. — (Высшее образование). — ISBN 978-5-534-07052-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/494255>.
2. Шиханова, Е. Г. Правовое регулирование инженерной деятельности : учебное пособие для вузов / Е. Г. Шиханова. — Москва : Издательство Юрайт, 2022. — 148 с. — (Высшее образование). — ISBN 978-5-534-13811-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496632>.
3. Правовая информатика : учебник и практикум для вузов / под редакцией С. Г. Чубуковой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 314 с. — (Высшее образование). — ISBN 978-5-534-03900-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/488822>.
4. Правовая статистика : учебник и практикум для среднего профессионального образования / И. Н. Андрюшечкина, Е. А. Ковалев, Л. К. Савюк, Ю. А. Бикбулатов ; под общей редакцией Л. К. Савюка. — Москва : Издательство Юрайт, 2022. — 410 с. — (Профессиональное образование). — ISBN 978-5-534-04991-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/491690>.
5. Рассолов, И. М. Информационное право : учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/488767>.

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/>
 - ЭБС РГБ <http://www.rsl.ru/>
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/>

- Ресурсы Института научной информации по общественным наукам Российской академии наук (ИНИОН РАН) <http://elibrary.ru>.
- Университетская информационная система РОССИЯ. <http://www.cir.ru/index.jsp>.
- Министерство экономического развития и торговли РФ <http://economy.gov.ru>
- Encyclopedia of Law and Economics <http://allserv.rug.ac.be/~gdegeest>
- Библиотечка Либертариума – <http://www.libertarium.ru/library>
- Материалы по социально-экономическому положению и развитию в России – <http://www.finansy.ru>
- Мониторинг экономических показателей — <http://www.budgetrf.ru>




Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля³:

1. Лабораторный практикум по дисциплине «Правовые основы кибербезопасности».
2. Сборник задач по дисциплине «Правовые основы кибербезопасности».

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

Оценочные материалы и балльно-рейтинговая система⁴ оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Правовые основы кибербезопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Доцент кафедры прикладной информатики и теории вероятностей Должность, БУП		С.А. Васильев Фамилия И.О.
РУКОВОДИТЕЛЬ БУП: Зав. кафедрой прикладной информатики и теории вероятностей Наименование БУП		К.Е. Самуйлов Фамилия И.О.
РУКОВОДИТЕЛЬ ОП ВО: Зав. кафедрой прикладной информатики и теории вероятностей Должность, БУП		К.Е. Самуйлов Фамилия И.О.

³- все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины в ТУИС

⁴ - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.