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

Факультет физико-математических и естественных наук
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИСТОЧНИКИ УГРОЗ КИБЕРБЕЗОПАСНОСТИ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

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)

2024 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Источники угроз кибербезопасности» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 5 семестре 3 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 5 разделов и 13 тем и направлена на изучение эффективных практик и технологий, используемых для защиты киберпространства.

Целью освоения дисциплины является Целью освоения дисциплины «Источники угроз кибербезопасности» является знакомство студентов с основами обеспечения кибербезопасности и формировании у них представлений о необходимости мер защиты в киберпространстве. Применение полученных знаний будет способствовать обоснованному выбору ими эффективных мер противодействия и механизмов обеспечения кибербезопасности хозяйствующих субъектов в соответствии с нормативно-правовой базой РФ и иных стран в области защиты информации и иных экономических систем

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Источники угроз кибербезопасности» 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)
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации и результатов исследований	ПК-1.1 Знает методы анализа и обобщения отечественного и международного опыта в соответствующей области исследования; ПК-1.2 Умеет применять методы анализа научно-технической информации для решения стандартных задач в собственной профессиональной и научно-исследовательской деятельности; ПК-1.3 Владеет базовыми навыками подготовки научных обзоров и (или) публикаций, рефератов и библиографий по тематике проводимых исследований на русском и иностранном языке;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	ПК-5.1 Знает методы организации 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-5.3 Умеет применять методы управления кибербезопасностью предприятий и иных экономических систем; 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-5.5 Владеет навыкками организации управления кибербезопасностью предприятий и иных экономических систем; ПК-5.6 Владеет навыками применения нормативно-правовой базы РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Источники угроз кибербезопасности» относится к блоку по выбору блока образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Источники угроз 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***
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации и результатов исследований		Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Анализ и показатели эффективности кибербезопасности предприятия; Кибербезопасность платежных систем; *Иностранный язык (дополнительные разделы)***; *Русский язык как иностранный (дополнительные разделы)***; *Практический курс иностранного языка***; *Практический курс русского языка (как иностранного)***;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем		Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Цифровая трансформация глобальной экономики; Киберполитика в международных экономических отношениях; Искусственный интеллект в бизнесе; Дизайн мышление; Защита сетей и кибербезопасность; Анализ и показатели

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
			эффективности кибербезопасности предприятия; Искусственный интеллект и кибербезопасность; Киберполигон; Кибербезопасность платежных систем; Технологии распределенного реестра Blockchain;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Источники угроз кибербезопасности» 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)**
			5
Контактная работа, ак.ч.	*54*		*54*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	36		36
Самостоятельная работа обучающихся, ак.ч.	*54*		*54*
Контроль (экзамен/зачет с оценкой), ак.ч.	*0*		*0*
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	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Введение, основные понятия угроз кибербезопасности	1.1	Основные определения: кибербезопасность и информационная безопасность, киберпространство и информационное пространство, киберинфраструктура, кибервоздействие, критически важное киберпространство и киберинфраструктура, обеспечение кибербезопасности, уязвимость кибербезопасности, угроза (риск) кибербезопасности, инцидент кибербезопасности. Классификация уязвимостей кибербезопасности по области происхождения, по типам недостатков ИС, по месту возникновения. Классификация угроз кибербезопасности: дерево систематической классификации киберугроз, связи между различными типами киберугроз, источники киберугроз. Классификация основных видов кибервоздействий	ЛК, СЗ
		1.2	Основные принципы противодействия угрозам кибербезопасности. Доктрина информационной безопасности РФ. Государственные стратегии кибербезопасности: ЕС, США, Канады, Японии. Руководство по кибербезопасности для развивающихся стран. Концепция стратегии кибербезопасности в РФ. Информационное противоборство. Основные критерии безопасности: готовность, целостность, конфиденциальность, идентификация, аутентификация, неотказуемость, физическая безопасность, решения по вопросам безопасности. Кибербезопасность киберфизических систем, кибербезопасность «Интернета-вещей»	ЛК
Раздел 2	Угрозы кибербезопасности открытого предприятия	2.1	Нарушения защиты на прикладном и сетевом уровнях. Общий обзор классификаций угроз безопасности: перечень наиболее опасных рисков информационной безопасности для веб-приложений по мнению экспертного сообщества (OWASP), классификация уязвимостей и недостатков программного обеспечения (CWE), классификация шаблонов компьютерных атак (CAPEC), классификация угроз безопасности веб-приложений (WASC)	ЛК, СЗ
		2.2	Несанкционированный доступ: несанкционированный доступ к компьютерным системам, сетям, информационным ресурсам и информации.	ЛК, СЗ
		2.3	Перехват данных: перехват и анализ сетевого трафика, перехват информации, аутентификация и перехват учетной записи, нелегальный перехват информационных ресурсов, перехват управления	ЛК, СЗ
		2.4	Технические каналы утечки информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок. Перехват побочных электромагнитных,	ЛК

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			акустических и других излучений устройств и линий связи. Наводки на вспомогательные технические средства	
Раздел 3	Анализ уязвимостей, меры противодействия и механизмы обеспечения безопасности	3.1	Идентификация уязвимых мест системы. Инспекция кода, fuzzing, анализ спецификаций и архитектуры, анализ потока данных - taint анализ, эксплуатация уязвимостей, поиск уязвимостей в бинарном коде ПО, техника Threat Hunting. Инструменты анализа и тестирования приложений - SAST, DAST, IAST, Mobile AST, RASP. Тестирование на проникновение. Моделирование атак кибератак на внутренние ресурсы и системы. Применение сканеров инфраструктуры, сканеров веб-приложений. Сканирование и анализ защищённости методом чёрного и белого ящика	ЛК
		3.2	Анализ вероятности угроз. Оценка последствий. Методы оценки риска, стандарт ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска – стандарт ISO/IEC 27005 -2011. Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021. Общая система оценки уязвимостей. Стандарт CVSS 3.0. Модель оценки рисков. Модель принятия решений. Выбор механизмов безопасности. Оценка вероятностей угроз с использованием сканеров безопасности	ЛК, СЗ
		3.3	Меры противодействия и механизмы обеспечения безопасности. Выявление существующих и потенциальных угроз в компьютерных сетях, анализ вероятности угроз, оценка последствий реализации угроз, оценка стоимости нарушения защиты и расчет стоимости мер противодействия, выбор механизмов и методов обеспечения безопасности, регистрация событий безопасности, обнаружение (предотвращение) вторжений, обеспечение целостности информационной системы и информации, обеспечение доступности информации. Идентификация и аутентификация субъектов доступа и объектов доступа, управление доступом субъектов доступа к объектам доступа, ограничение программной среды, антивирусная защита, контроль (анализ) защищенности информации. Тестирование на проникновение. Перенаправление вредоносного трафика. Мониторинг систем защиты. Анализ и реагирование на инциденты кибербезопасности. Оценка эффективности систем защиты. Управление уязвимостями. Физическая защита при развертывании и эксплуатации сетей. Обеспечение безопасности приложений, серверов, конечных пользователей, защита среды виртуализации, защита технических средств, защита информационной системы, ее средств и систем связи и передачи данных. Защита от атак методами социальной инженерии. Использование баз уязвимостей и	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			угроз	
Раздел 4	Архитектура безопасности инфокоммуникационной среды предприятия	4.1	Обеспечение сквозной безопасности. Ключевые аспекты безопасности. Понятие факторов безопасности. Контроль доступа, аутентификация, неотказуемость, конфиденциальность данных, безопасность связи, целостность данных, доступность, секретность. Понятие уровней безопасности. Уровень безопасности инфраструктуры, уровень безопасности услуг, уровень безопасности приложений. ¶	ЛК
Раздел 5	Организации защиты безопасности сети	5.1	Защита сетей LAN. Угрозы безопасности локальных сетей. Безопасность сетевого оборудования. Безопасность оконечного оборудования. Контроль состояния защищенности. Демилитаризованная зона. VPN, TLS, сегментация беспроводных сегментов, защита периметра межсетевыми экранами.	ЛК, СЗ
		5.2	Подходы к организации защиты беспроводных сетей. Компьютерные сети стандарта 802.11. Способы защиты данных в беспроводных сетях стандарта IEEE 802.11. Алгоритмы шифрования стандарта в беспроводных сетях IEEE 802.11. Использование механизмов защиты LAN для обслуживания WLAN	ЛК, СЗ
		5.3	Удаленный доступ. Защита удаленного офиса. Инфраструктура виртуальных рабочих столов (VDI), RDP/RDS	ЛК, СЗ

* - 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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог.
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог.

	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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams или аналог.

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181222 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей.

2. Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей.

3. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. — Вологда : Инфра-Инженерия, 2020. — 692 с. — ISBN 978-5-9729-0486-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148383 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

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

1. Курс лекций по дисциплине «Источники угроз кибербезопасности».

Дополнительная литература:

1. Сэрра, Э. Кибербезопасность: правила игры. Как руководители и сотрудники влияют на культуру безопасности в компании / Э. Сэрра. — Москва : Альпина Паблишер, 2022. — 192 с. — ISBN 978-5-907534-38-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/213989 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

2. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус. — Вологда : Инфра-Инженерия, 2020. — 644 с. — ISBN 978-5-9729-0512-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/148386 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

3. Чио, К. Машинное обучение и безопасность : руководство / К. Чио, Д. Фримэн ; перевод с английского А. В. Снастина. — Москва : ДМК Пресс, 2020. — 388 с. — ISBN 978-5-97060-713-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131707 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

4. Информационный портал по безопасности — URL: https://www.securitylab.ru

5. Интернет-портал по информационной безопасности в сети — URL: https://safe-surf.ru

6. Федеральный закон РФ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ.

7. Федеральный закон РФ "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

8. ГОСТ Р ИСО/МЭК 27033-4 – 2021 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей

9. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

10. Стратегия национальной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 2 июля 2021 г. N 400

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 «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/

* - 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 «Источники угроз кибербезопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

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

РАЗРАБОТЧИК:

Доцент кафедры теории вероятностей и кибербезопасности		Ботвинко Анатолий Юрьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*