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

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ
(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)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Технологии обеспечения кибербезопасности предприятий» 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 4 разделов и 17 тем и направлена на изучение основных концепций и методов обеспечения кибербезопасности предприятий.

Целью освоения дисциплины является получение обучающимися знаний об основных технологиях и методах управления кибербезопасностью экономических субъектов. Усвоение курса позволит принимать эффективные управленческие решения в деятельности предприятий и организаций, иных экономических субъектов в условиях растущих угроз кибербезопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Технологии обеспечения кибербезопасности предприятий» 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-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	ПК-4.1 Знает языки визуального моделирования; ПК-4.2 Умеет анализировать и оценивать факторы и условия, влияющие на принятие управленческих решений; ПК-4.3 Умеет проводить оценку эффективности принятия решения в соответствии с выбранными критериями или выбранными целевыми показателями;
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 «Технологии обеспечения кибербезопасности предприятий» 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 «Технологии обеспечения кибербезопасности предприятий».

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-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	Микроэкономика; Макроэкономика; Архитектура и ИТ-инфраструктура предприятия;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Моделирование бизнес-процессов; Рынки информационно-коммуникационных технологий и Индустрия 4.0; Искусственный интеллект и кибербезопасность; Финансовая безопасность;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем		Цифровая трансформация глобальной экономики; Киберполитика в международных экономических отношениях; Анализ и показатели эффективности кибербезопасности предприятия; Искусственный интеллект и кибербезопасность; Кибербезопасность платежных систем; Технологии распределенного реестра Blockchain; Финансовая безопасность; Практикум по кибербезопасности предприятия; Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Технологии обеспечения кибербезопасности предприятий» составляет «4» 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.	*63*		*63*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

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	Криптографические методы защиты информации	1.1	Классификация криптографических алгоритмов	ЛК, СЗ
		1.2	Схема Фейстеля	ЛК, СЗ
		1.3	Шифры DES и 3DES.	ЛК, СЗ
		1.4	Шифр AES	ЛК, СЗ
		1.5	Шифр ГОСТ 28147-89. Шифры «Кузнечик», «Магма». Режимы работы блочных шифров	ЛК, СЗ
		1.6	Основные принципы построения потоковых шифров	ЛК, СЗ
		1.7	Потоковый шифр RC4	ЛК, СЗ
		1.8	Распределение ключей по схеме Диффи–Хеллмана	ЛК, СЗ
		1.9	Криптографическая хэш-функция и цифровая подпись. Электронная цифровая подпись по ГОСТ 34.10-2018. Криптографическая хэш-функция. Криптографическая хэш-функция по ГОСТ 34.11-2018	ЛК, СЗ
Раздел 2	Технологии контроля доступа для защиты сетевой инфраструктуры предприятия	2.1	Классификация межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам	ЛК, СЗ
		2.2	Обобщённый процесс обработки сетевого трафика межсетевыми экранами	ЛК, СЗ
		2.3	Виртуальные частные сети (VPN)	ЛК, СЗ
		2.4	Идентификация и аутентификация	ЛК, СЗ
Раздел 3	Антивирусная защита, аудит и мониторинг	3.1	Архитектура систем обнаружения атак. Приказ ФСБ РФ от 06.05.2019 № 196. Рекомендации по созданию корпоративных и ведомственных центров ГосСОПКА	ЛК, СЗ
		3.2	Управление компьютерными инцидентами информационной безопасности	ЛК, СЗ
		3.3	Меры обеспечения информационной безопасности и цели их применения согласно ГОСТ Р ИСО/МЭК 27001:2021	ЛК, СЗ
Раздел 4	Мониторинг информационной безопасности	4.1	Мониторинг информационной безопасности. Уровни мониторинга ИБ. ГОСТ Р 59547-2021	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 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. Ботвинко Анатолий Юрьевич. Технологии обеспечения кибербезопасности предприятий. учебное пособие [Электронный ресурс]. - М. : РУДН, 2023. 95 с. ISBN 978-5-209-11758-2 URL: https://mega.rudn.ru/MegaPro/UserEntry?Action=Link_FindDoc&id=516017&idb=0

2. 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

3. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242 (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

4. Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз ; перевод с английского А. В. Добровольская. — Москва : ДМК Пресс, 2020. — 308 с. — ISBN 978-5-97060-649-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131682 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

5. 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

6. Гродзенский, Я. С. Информационная безопасность : учебное пособие / Я. С. Гродзенский. — Москва : Проспект, 2020. — 142 с. — ISBN 978-5-9988-0845-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181193 (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

7. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А.

Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

8. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/207095 (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

Дополнительная литература:

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111053 (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

2. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 2-е изд. — Москва : МГТУ им. Н.Э. Баумана, 2018. — 250 с. — ISBN 978-5-7038-4899-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172839 (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

3. Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111075 (дата обращения: 16.04.2022). — 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. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Основные положения

7. ГОСТ Р 59383—2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом

8. ГОСТ Р (проект, первая редакция) Управление инцидентами, связанными с безопасностью информации. Руководство по реагированию на инциденты в сфере информационных и компьютерных технологий (ISO/IEC 27035-3:2020, NEQ)

9. ГОСТ 34.10 – 2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

10. ГОСТ Р ИСО/МЭК 27004 – 2021. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание (ISO/IEC 27004:2016, IDT)

11. ГОСТР ИСО/МЭК 27033-4 – 2021 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей

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 https://mega.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 «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы

- Sage https://journals.sagepub.com/
- Springer Nature Link https://link.springer.com/
- Wiley Journal Database https://onlinelibrary.wiley.com/
- Наукометрическая база данных Lens.org https://www.lens.org

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

1. Курс лекций по дисциплине «Технологии обеспечения кибербезопасности предприятий».

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

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:

Должность, БУП	*Подпись*	*Фамилия И.О.*